HIPAA MANUAL
February 2003

This manual was compiled by the Alcohol and Drug Abuse Division HIPAA Workgroup during the summer and fall of 2002. It was modified by Colorado Mental Health Services in February 2003. It contains detailed information about the Privacy Rule and summary information about the Codes and Transaction Rule. In an effort to simplify very complex rules the workgroup has focused on provider-specific issues. Many parts of many sections have been purposefully left out of this manual because they do not apply to provider-specific issues (e.g., specifics for Health Plans). A complete copy of both the HIPAA Privacy Rule (Attachment B) and the Codes and Transactions Rule are included (Attachment C) at the end of this document, and all users of this manual should read both in their entirety. Because other HIPAA rules were still pending final publication at the time this manual was completed, they are not fully addressed in this document.

DISCLAIMER

This document is provided for general educational and informational purposes only and should not be construed as legal advice. Parties using this tool should consult professional legal counsel for legal advice. The provision of these materials for the stated purpose is not intended to assert any guarantee of HIPAA compliance and does not denote an endorsement or recommendation of any materials by the Colorado Department of Human Services (CDHS) or any of its agencies or employees.

Many of the attachments to this manual are copies of materials available to the public on the World Wide Web. Web addresses and author citations have been included whenever possible.

PURPOSE

The purpose of this manual is to inform providers about HIPAA and to assist them in their efforts towards HIPAA compliance. It was compiled specifically for covered entity "providers."

AVAILABILITY

This manual is available in paper copy from the Colorado Mental Health Services at 3824 W. Princeton Circle, Denver, CO 80236, 303-866-7417. There is a cost for copying. All attachments are included with the paper copy. It is also available free of charge on the MHS web site at http://www.cdhs.state.co.us/ohr/mhs. Note that all attachments are separate documents that must be downloaded.

TABLE OF CONTENTS

Overview of HIPAA

The Purpose of HIPAA

In 1996 Congress passed the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) to improve the efficiency and effectiveness of the nation's health care system. (A copy of this Act is included in this manual.)

HIPAA requires the federal Department of Health and Human Services (DHHS) to establish certain national standards to simplify the coding of health care transactions and to ensure the privacy and security of individually identifiable health information.

HIPAA's Standards

There are 9 HIPAA Standards, 8 of which are or will be implemented. One standard, the National Individual Identifier is on indefinite hold.

1. **Electronic Transaction and Code Sets**
   This regulation adopts national standards for 8 electronic transactions and for uniform codes for diagnosis, treatment, medication, dental services, and medical supplies. It eliminates the use of local procedure codes. The 8 electronic transactions are:
   - health care claims or encounters
   - eligibility for a health plan
   - referral certifications or authorizations
   - health care claim status
   - enrollment and disenrollment in a health plan
   - health care payment and remittance advice
   - health plan premium payments
   - coordination of benefits

2. **Privacy**
   This regulation establishes standards for the use and disclosure of protected health information, and for patient rights including access to health care records.

3. **Security**
   This regulation addresses the physical and technical security requirements necessary to guard the integrity, confidentiality and availability of individual health information that is collected, stored, maintained or transmitted.

4. **National Provider Identifier**
   This regulation is intended to standardize and simplify provider identifiers through the use of the Medicare National Provider System.

5. **National Employer Identifier**
   This regulation is intended to standardize and simplify employer identifiers through the use of the IRS tax identification system.

6. **National Health Plan Identifier**
   This regulation is intended to standardize and simplify Health Plan identifiers through a process to be determined.

7. National Individual Identifier
This regulation is on indefinite hold. It was intended to give each individual a unique identifier for all health care use.

8. Claims Attachment
Information about this standard has not yet been published.

9. Enforcement
Information about this standard has not yet been published.

HIPAA Compliance Due Dates

STANDARD	Notice of Proposed Rule Making Status	Final Rule Status	Compliance Required
Electronic Transaction and Code Sets	published 5/7/98	published 8/17/00 modified 5/31/02	10/16/02 unless compliance plan for deferment submitted by 10/16/02; then 10/16/03
Privacy	published 11/3/99	published 12/28/00 modified 8/14/02	4/14/03
Security	published 8/12/98	Published 2/20/03	4/21/05
National Provider Identifier	published 5/7/98	not yet published	10/16/02
National Employer Identifier	published 6/16/01	not yet published	10/16/02
National Health Plan Identifier	not yet published	not yet published	10/16/02
National Individual Identifier	not yet published	on hold	on hold
Claims Attachment	not yet published	not yet published	10/16/02
Enforcement	not yet published	not yet published	4/14/03

HIPAA and Other Laws
In summary, HIPAA may not supercede or negate other laws. HIPAA mandates that when comparing it to other laws, you follow whichever part of either is the most stringent, (i.e., provides the individual and their health information with the greatest protection).

1. **For state law**, see section 160.203.

2. **HIPAA and the Duty to Warn**

HIPAA recognizes that clinicians have a duty to warn [for detail see the actual Privacy Rule, section 164.512 (j)] when a serious, imminent threat exists to the health or safety of an individual or the public. HIPAA couches this in terms of applicable laws and standards of ethical conduct.

The Tarasoff Versus the Regents of the University of California case, decided by the California Supreme Court, established the parameters for clinicians regarding the duty to warn, and to whom disclosure about an impending threat should be made. In 1986 the State of Colorado codified this case law with C.R.S. 13-21-117, outlining the conditions under which mental health providers have a specific duty to warn or protect individuals from threats of physical violence made by a client.

Why Should I Care About HIPAA?

1. Whether or not you have identified yourself as a "covered entity," consider complying. HIPAA is fast becoming the national standard for privacy and confidentiality of health care related information.

2. HIPAA mandates that providers educate their clientele about the Privacy Rule. Consumers are becoming more informed about their rights and provider responsibilities. You need to be as informed about it as your consumers.

3. A great portion of the HIPAA Privacy Rule offers basic protection for sensitive, confidential information.

4. There are penalties (financial and imprisonment) that may be levied against those who are supposed to comply with HIPAA but don't.

Determining if you're affected by HIPAA

If you answer "yes" to any of the following questions, your organization may be impacted by HIPAA.

1. Are you a covered entity?

"Covered entity" means:

- a health plan (example: Health Maintenance Organization)
- a health care clearinghouse (examples: billing service, community health management information system, or health care re-pricing company)
- a health care provider (examples: physicians, psychologist, clinic, hospital, alcohol and substance abuse treatment provider) that transmits any health information related to HIPAA "transactions" in electronic form.

"Electronic Transmission" means the sharing of information between two parties to carry out financial or administrative activities related to health care by electronic media including:

- the Internet

- an Extranet (using Internet technology to link a business with information only accessible to collaborating parties)
- leased lines
- dial-up lines
- private networks
- magnetic tape or compact disk if physically moved from one location to another

"HIPAA Transactions" means:

- health care claims or equivalent encounter information
- health care payment and remittance advice
- coordination of benefits
- health care claim status
- enrollment and disenrollment in a health plan
- eligibility for a health plan
- health plan premium payments
- referral certification and authorization
- first report of injury
- health claims attachments
- other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation

2. Is your organization considered a Business Associate of a covered entity?

"Business Associate" means:

Someone who performs a function on behalf of a covered entity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, data processing, utilization review, quality assurance, billing, benefits management, practice management, and re-pricing;

OR

Someone who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, that involves the use or disclosure of individually identifiable health information.

"Individually Identifiable Health Information" means any information that is:

- Created or received by a health care provider, health plan, employer or health care clearinghouse; and
- Relates to the physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual; and
- Identifies or may be used to identify an individual.

Data elements that make health information individually identifiable include: name, address, employer, relatives' names, date of birth, telephone and fax numbers, e-mail addresses, IP addresses, social security numbers, medical record numbers, member or account number, certificate/license number, voice/fingerprints, photos, or other number, code or characteristics.

3. **Does your organization regularly handle individually identifiable health information?**

4. **Does your organization store or transmit individually identifiable health information in an electronic form in connection with a "HIPAA" transaction?**

If you responded "yes" to any of the above, your organization may be impacted by HIPAA. Seek legal counsel to determine how your business may be specifically affected.

HIPAA
Privacy Rule

Section 160.203 General rule and exceptions

What you need to know:

HIPAA preempts State law except when
a) The Secretary determines State law is necessary to
1) prevent fraud and abuse providing or paying for health care
2) ensure State regulation of insurance and health plans
3) report on health care delivery or costs (State reporting)
4) serve a compelling need related to public health, safety or welfare
5) regulate controlled substances
b) the State law relates to privacy of individually identifiable health information and is more stringent that HIPAA
c) the State law provides for public health activities (disease or injury, child abuse, birth or death reporting, or public health surveillance, investigation or intervention)
d) the State law requires health plans to report or allow access to information for management/financial audits, program monitoring/evaluation, licensure or certification of facilities or individuals.

What you need to do:

If you are unsure of whether or not HIPAA preempts a specific State law, seek professional legal counsel.

HIPAA
Privacy Rule

Section 160.310 Responsibilities of covered entities

What you need to know:

1. You must keep records and submit reports about compliance to HIPAA to the Secretary of Health and Human Services or his/her designee if the Secretary needs to determine that you are/are not compliant.

2. You must cooperate with the Secretary/designee if he/she investigates your compliance to HIPAA.

3. You must permit the Secretary/designee access to information
    a) during normal business hours to facilities, books, records, accounts, protected health information, etc.; if the Secretary/designee suspects you hare/are destroying or hiding any documents, the Secretary has the right to access at any time without notice.
    b) that may be in the exclusive possession of another entity, and you must certify what efforts you made to obtain this information.
    c) the Secretary may not disclose any protected health information you provide except if necessary to ascertain or enforce compliance with HIPAA.

What you need to do:

1. If you are a covered entity or business associate, comply with the Privacy Rule of HIPAA.

2. Cooperate with the Secretary during any investigation and provide access to any and all documents required.

3. For the investigation, try to obtain and document your efforts in obtaining documents the Secretary needs that may have become the exclusive possession of another entity (example: a referral form you sent to another provider about a specific client).

HIPAA
Privacy Rule

Section 164.502 Uses and disclosures of protected health information: general rules

What you need to know:

1. **You MAY disclose protected health information:**
   a) to the individual
   b) for treatment, payment or health care operations (See Section 164.506)
   c) with a valid authorization (See Section 164.508)
   d) when agreed to by the individual (See Section 164.510)
   e) when disclosures are required by law (See Section 164.512 and 164.514)

2. **You ARE REQUIRED to disclose protected health information:**
   a) when required by law (See Section 164.512 and 164.514) and
   b) to the Secretary to determine compliance or for an investigation (See Section 160.310)

3. **Minimum necessary**
   When disclosing protected health information you must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request, unless:
   a) disclosure is to a health care provider for treatment;
   b) disclosure is to the individual;
   c) disclosure is made pursuant to an authorization;
   d) disclosure is to the Secretary to determine compliance or for an investigation;
   e) disclosure is required by law.

4. **De-identification**
   You may create information that is de-identified and that cannot be used to identify an individual. See Section 164.514 for more information for what constitutes "de-identified information." Use of codes that permit de-identified information to be re-identified constitutes a disclosure of protected health information.

5. You may disclose protected health information to a business associate if you obtain satisfactory assurance that business associate will appropriately safeguard the information. You MUST document this through a written business associate contract. (See Attachment D.)

6. You must comply with these requirements even for deceased individuals, see section 164.512(g).

7. **Working with personal representatives**
   You must treat a personal representative as the individual for the purposes of this section. To determine who is and isn't considered a personal representative, and for more detail about adults, emancipated minors and unemancipated minors, see HIPAA Privacy Rule, Section 164.502 (g). (This part is complex and cannot be summarized.)

8. You must comply with these requirements when communicating protected health information.

9. If you are required to have a notice (see Section 164.520) you must use protected health information in a manner consistent with this notice.

10. **Disclosure by whistleblowers is allowed if:**
a) the workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or if the care, services or conditions potentially endangers on or more patients, workers or the public, and
b) the disclosure is to a health oversight agency or public health authority authorized by law to investigate or oversee the conduct or conditions of the covered entity, or to an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining legal options related to this disclosure.

11. **Disclosure by workforce members who are victims of a crime is allowed if:**
a) it is a disclosure to a law enforcement official about the suspected perpetrator of the criminal act, and
b) it is limited to the information listed in Section 164.512.

HIPAA
Privacy Rule

Section 164.504 Uses and disclosures: Organizational requirements

What you need to know:

1. **If you are a hybrid-entity,**
   a) HIPAA applies only to the health care components and to protected health information that is created or received by or on behalf of the health care component of the entity.
   b) A person who performs duties for both the health care component and another component of the entity must comply with HIPAA..

2. Legally separate covered entities that are affiliated may designate themselves as a single covered entity if all are under common ownership or control and the affiliation is documented as required by Section 164.530. Affiliated covered entities must comply with HIPAA.

3. **Business Associate Contracts**
   If you and your business associate are NOT governmental entities, You MUST have formal, written contracts with business associates. (See Attachment D.)
   A Business Associate Contract
   a) establishes the permitted and required uses and disclosures by the business associate.
   b) permits the business associate to use and disclose protected health information for the proper management and administration of the business associate
   c) permits the business associate to provide data aggregation services for the covered entity.
   d) states the business associate will
      1) not use or further disclose information other than as permitted or required by the contract or law
      2) use appropriate safeguards to prevent use or disclosure of the information
      3) report to the covered entity any use or disclosure not provided for in its contract
      4) ensure than any agent or subcontractor also agrees to the same restrictions and conditions of a business associate contract
      5) apply by the terms of HIPAA, including making its operation, books and records available to the Secretary
      6) upon termination, if feasible, return or destroy <u>all</u> protected health information received from, created by or received by the business associate on behalf of the covered entity
   e) authorizes termination of the contract if the covered entity has determined the business associate has violated a material term of the contract.
   f) permits the business associate to use the information for the proper management and administration of the business associate, and to carry out its legal responsibilities.
   g) permits the business associate to disclose the information if the disclosure is required by law or if the business associate obtains reasonable assurances from the person to whom the information is to be disclosed that it will be held

confidentially and used or further disclosed only as required by law or for the specific purpose for which it was disclosed to the person, and the person notifies the business associate of any breaches of confidentiality of this information.

4. You MUST terminate a Business Associate Contract if that business associate is not in compliance with HIPAA, unless they have taken reasonable and successful steps to cure the breach or end the violation. If termination is not possible, you MUST report the problem to the Secretary.

5. **A Memorandum of Understanding**
If you and your business associate are both governmental entities, a memorandum of understanding that includes all the terms of a business associate contract may replace the contract itself. If the business associate is required by law to provide a service to the covered entity, the covered entity may comply with legal mandate regarding disclosure of protected health information provided it attempts in good faith to obtain satisfactory assurances the business associate will comply with HIPAA, or documents its attempt and the reasons such assurances cannot be obtained.

What you need to do:

1. If you are a hybrid-entity, partition off that part of your business that deals with protected health information and assure that part complies with HIPAA.

2. Write, have all parties sign and file business associate contracts or memorandums of understanding (used only between two governmental entities) with all entities with whom you do business who meet the definition of Business Associate (See Definitions.)

HIPAA
Privacy Rule

Section 164.506 Uses and disclosures to carry out treatment, payment or health care operations

What you need to know:

1. You may obtain consent from the individual to use or disclose protected health information to carry out your treatment, payment or health care operations without an authorization (see Section 164.508).

2. If an authorization is required, then a consent is not effective to permit use or disclosure of protected health information. You must also have an authorization.

3. You may disclose protected health information for treatment activities of another covered entity.

4. You may disclose protected health information to another covered entity or health care provider for the payment activities of the entity that receives the information.

5. You may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information if you and the other entity both have or had a relationship with the individual, the protected health information pertains to this relationship, and the disclosure is for
a) conducting quality assessment and improvement or provider reviewing and training activities as identified in #1 and #2 of the Health Care Operations definition (See definitions.) or
b) for the purpose of health care fraud and abuse detection or compliance.

6. You may disclose protected health information to another covered entity if you and this covered entity both participate in an organized health care arrangement for health care operation activities of the organized health care arrangement. (See Organized Health Care Arrangement in definitions.)

HIPAA
Privacy Rule

Section 164.508 Uses and disclosures for which an authorization is required

What you need to know:

1. **Use of authorizations**
In order to use or disclose protected health information, you MUST use an authorization (See Attachment G) for use and disclosure of:
a) psychotherapy notes, except
1) for use by the originator of the notes for treatment;
2) for use or disclosure for your own training programs in which students learn under supervision to practice or improve their skills in counseling;
3) for use of disclosure by the covered entity to defend a legal action or other proceeding brought by the individual;
4) when required by the Secretary to investigate or determine compliance (See Section 160.310);
5) to the extent required by law ;
6) for uses and disclosures for health oversight activities (See Section 164.512)
7) for coroners and medical examiners (See Section 164.512);
8) when such is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public (See Section 164.512).
b) marketing - a face-to-face marketing communication by the covered entity to an individual, or a marketing promotional gift of nominal value provided by the covered entity. If marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

2. **Content of an authorization**
A valid authorization must be written in plain language and contain the following. It may also contain additional elements or information if they are consistent with the required elements.
a) a description of the information to be used;
b) the name or other specific identification of the person(s), or class of persons authorized to make the requested disclosure or use;
c) the name or other specific identification of the person(s) or class of persons to whom you are allowed to make the disclosure or use;
d) a description of each purpose of the requested disclosure or use. "At the request of the individual" is sufficient only when the individual initiates the authorization and does not provide a reason for it.
e) the expiration date or event after which you may not disclose the information;
f) signature of the individual and date of signature. If the authorization is signed by a personal representative of the individual that person's authority to act should be included at the signature line.
g) a statement that the individual has the right to revoke the authorization in writing, and whether or not treatment or payment are conditioned on the existence of such authorization.

3. **Invalid authorizations**
Defective authorizations are invalid. Defects include:
a) the expiration date has passed or the expiration event has occurred;
b) the authorization is incomplete;
c) the authorization is known by the covered entity to have been revoked;
d) any material in the authorization is known by the covered entity to be false;
e) a condition is placed on the authorization (except for research-related treatment or enrollment in or eligibility for benefits in a health plan prior to the individual's enrollment in the health plan).

4. An authorization may <u>not</u> be combined with any other document to create a compound authorization except:
    a) for a research study;
    b) for psychotherapy notes unless combined with another authorization for a use or disclosure of psychotherapy notes.

5. A provider cannot condition the provision of treatment or payment on the existence of an authorization except for research. If you are creating protected health information solely for the purpose of disclosing it to a third party (e.g., a referral provider) you may condition the provision of health care on the existence of an authorization.

6. **Revoking an authorization**
The individual may revoke in writing an authorization at any time except to the extent that authorization has already been acted upon, or if it was obtained as a condition of obtaining insurance coverage.

<u>What you need to do:</u>

1. You must use an authorization (see Attachment G) for each client.

2. You must create an authorization form that includes HIPAA language and is appropriate for your practice.

3. You must document and retain all signed authorizations in your client files.

4. You must comply with the individual's written request to revoke an authorization.

5. You must provide a copy of the signed authorization to the individual is you are the one requesting an authorization be created.

HIPAA
Privacy Rule

Section 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

What you need to know:

1. You may use or disclose protected health information provided you inform the individual in advance, you provide an opportunity for that person to agree or object, and you infer from the circumstances that the individual does not object to the disclosure.

2. **When the individual is not present**
   In an emergency situation in which the client cannot agree to the use or disclosure, you may, in the exercise of professional judgment, disclose information directly related to your care of the individual if you have determined that it is in the best interests of the individual.

3. **For disaster relief**
   You may use or disclose protected health information to a public or private entity authorized by law or its charter to assist in disaster relief efforts during an emergency if the individual agrees, or if the individual is not present and you determine that use or disclosure is in the best interests of the individual.

What you need to do:

1. Inform your clients in advance in writing of all expected or possible uses or disclosures of their protected health information and obtain their written approval.

2. Document thoroughly the circumstances for any use or disclosure during an emergency when the individual is not present or has not agreed in advance to such a disclosure.

HIPAA
Privacy Rule

Section 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required

What you need to know:

1. **Disclosures without an opportunity to agree or object**

You may use or disclose protected health information without offering the client an opportunity to agree or object when:

a) such use or disclosure is required by law;

b) it is required for public health activities to a public health authority, including:

1) it is required to report child abuse or neglect to a public health or other appropriate government authority;

2) it is required to track or report adverse events to the FDA related to FDA-regulated products or activities;

c) it is about victims of abuse, neglect or domestic violence

1) if you reasonably believe the individual is a victim of abuse, neglect or domestic violence, you may report such to an agency authorized by law to receive such reports;

2) if you believe the disclosure is necessary to prevent serious harm to the individual or their potential victims, and that waiting to obtain the individual's consent would materially and adversely affect events. After reporting, you must inform the individual of such report unless:

a. in the exercise of your professional judgment you believe informing him/her would place that person at risk of serious harm, or

b. you would be informing the individual's personal representative, whom you believe is responsible for the abuse, neglect or injury.

d) it is to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative or criminal investigations, proceedings or actions; inspections; licensure or disciplinary action; or it is related to an investigation of claims for public health benefits not related to health;

e) it is for judicial or administrative proceedings in response to a court order or subpoena, discovery request or other lawful process and the party requesting such information has either obtained approval from the individual or has made a good faith attempt to provide written notice with opportunity to object to the individual and time for objection has elapsed. (This section is quite complex. For detail, please read Section 164.512 [e].)

f) it is for law enforcement purposes to a law enforcement official to identify or locate a suspect, fugitive, material witness or missing person, and if it is in compliance with

1) a court-ordered warrant, subpoena or summons issued by a judicial officer;

2) a grand jury subpoena; or

3) an administrative request including subpoena or summons, a civil or an authorized investigative demand, or similar process, and the information requested is relevant and material to the inquiry, the request is specific and limited in scope, and de-identification could not be reasonably used.

g) it is about an individual who died, to a law enforcement official and there is a suspicion that the death resulted from criminal conduct;
h) you believe in good faith that the individual committed a crime on the premises, to a law enforcement official;
i) it is for research purposes, provided that an Institutional Review Board or privacy board has approved and documented the waiver of authorization. (Research is a complex subject. Please read detail in Section 164.512 (i).)
j) it is to avert serious threat to health or safety;
k) it is for specialized governmental functions.

2. **Permitted disclosures for law enforcement purposes**
You may only disclose the following:
a) Name and address;
b) Date and place of birth;
c) Social security number;
d) Blood type and Rh factor;
e) Type of injury;
f) Date and time of treatment;
g) Date and time of death; if applicable; and
h) A description of distinguishing physical characteristics

3. **Permitted disclosures for victims of a crime**
You may disclose protected health information in response to a request by a law enforcement official if:
a) the individual agrees to the disclosure; or
b) you are unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
    1) the information is needed to determine whether a violation of law by someone other than this individual occurred, and such information is not intended to be used against the victim;
    2) immediate law enforcement activity dependent upon the information would be adversely affected by waiting until the individual could agree to disclosure; and
    3) you have determined that the disclose is in the best interests of the individual.

4. **Workmen's Compensation**
If for Workmen's Compensation cases you provide health care to the individual at the request of the individual's employer, and you are evaluating whether the individual has a work-related illness or injury, you must inform the individual about such possible disclosure in writing at the beginning of your care.

<u>What you need to do:</u>

1. In Workmen's Compensation cases, provide the client with a written notice that information may be shared with the employer.
2. In all cases, provide the client with a document that identifies the circumstances under which you must share protected health information and to whom, without first obtaining the client's consent.

3. For greater detail, read this section of the Rule, especially if you are involved in disclosure related to legal or law enforcement functions, research or military/government activities.

HIPAA
Privacy Rule

Section 164.514 Other requirements relating to uses and disclosures of protected health information.

What you need to know:

1. **De-identified health information**
   Protected health information is considered "de-identified" when the following are removed:
   a) name
   b) all geographic subdivisions smaller than State (e.g., street address, city, county, precinct, zip code, geocodes ,)
   c) all elements of date except year, for birth date, admission date, discharge date, date of death and all ages over 89
   d) telephone numbers
   e) fax numbers
   f) e-mail addresses
   g) social security numbers
   h) medical record numbers
   i) health plan beneficiary numbers
   j) account numbers
   k) certificate/license numbers
   l) vehicle identifiers, license plate, etc.
   m) device identifiers and serial numbers
   n) Web Universal Resource Locators (URLs)
   o) Internet Protocol (IP) addresses
   p) biometric identifiers including finger and voice prints
   q) full face photographic images
   r) any other unique identifying number, characteristic or code

2. **Use of unique identifiers or codes**
   You may assign a code as a means to identify client records provided that
   a) the code is not derived from any information about the individual and cannot be used to identify the individual; and
   b) you don't use the code for any other purpose or disclose it as a mechanism for individual identification.

3. **Role-based access**
   You must identify:
   a) those persons or classes of person in your workforce who need access to protected health information to carry out their duties; and
   b) the specific protected health information each person or class may have access to, and under what conditions.
   (See Attachment H)

4. You must make reasonable efforts to limit access of protected health information to that identified in #3 above.

5. **Minimum necessary**

You must limit the amount of protected health information disclosed to the minimum necessary to achieve the purpose of the disclosure.

6. **Limited data set**

You may use or disclose a "limited data set" only if you have a data use agreement in place (see Attachment F) with the recipient of the limited data set, and it is for the purposes of research, public health or health care operations only. A "limited data set" is protected health information that excludes direct identifiers of the individual or the relatives, employers or household members of the individual, including:

a) name
b) postal address other than town or city, State and zip code
c) telephone numbers
d) fax numbers
e) e-mail addresses
f) social security numbers
g) health plan beneficiary numbers
h) account numbers
i) certificate/license numbers
j) vehicle identifiers and serial numbers, including license plate numbers
k) device identifiers and serial numbers
l) web universal resource locators (URLs)
m) internet protocol (IP) addresses
n) biometric identifiers including finger and voice prints
o) full face photographs or comparable images.

7. **Uses and disclosures for fundraising**

You may use or disclose to a business associate the following without an authorization:

a) demographic information relating to an individual; and
b) dates of health care provided to an individual.

In any fundraising materials you send to individuals you must include a description of how they may opt out of receiving any further fundraising communications, and then assure that they are not sent such materials in the future.

8. **Verification requirements**

Prior to any disclosure you must exercise professional judgment to:

a) verify that the person receiving the information has the authority for such access to information;
b) obtain written, dated and signed documentation from the person requesting the information when document is required for disclosure (example: subpoena or similar process);
c) verify the identity of the requestor when the disclosure is to a public official or person acting on behalf of a public official (example: ID badge, proof of government status, letterhead, memorandum of understanding, purchase order, etc.); and
d) verify in a written statement the legal authority under which the information is requested.

What you need to do:

1. Complete the Information Flow Assessment Questionnaire (see Attachment H) for each person in your workforce, including yourself. You must identify:
   a) those persons or classes of person in your workforce who need access to protected health information to carry out their duties; and
   b) the specific protected health information each person or class may have access to, and under what conditions.

2. Use this completed questionnaire to create policies to limit access for persons or classes of persons in your workforce as appropriate.

3. Implement these policies in your workplace, including periodic measures to check to make sure the policies remain implemented.

4. File a copy of this completed questionnaire and associated policies.

5. If someone on your workforce does not have access to specific protected health information, you must reasonable efforts to make sure that information is not accessible to that individual. Document all measures you take to assure this.

6. If you are using or sharing identifiable protected health information, make sure you have the appropriate business associate contracts and/or memoranda of understanding in place, and client authorizations to permit this.

7. If you have a computerized data system, you may need to make adjustments to it to limit access at various levels for specific personnel.

8. Always limit the amount of information disclosed to the minimum necessary to accomplish the purpose of the disclosure. Make sure your written policies include this as a standard.

9. Review all requests for disclosure on an individual basis to assure you are only asking for or receiving the minimum necessary information.

10. If you disclose a “limited data set” make sure you have a formal data use agreement with the recipient of the disclosure on file.

11. If you know of a material breach or violation of the data use agreement you must take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, you must discontinue disclosure and report the problem to the Secretary.

12. Prior to any disclosure you must exercise professional judgment to:
    a) verify that the person receiving the information has the authority for such access to information;
    b) obtain written, dated and signed documentation from the person requesting the information when document is required for disclosure (example: subpoena or similar process);
    c) verify the identity of the requestor when the disclosure is to a public official or person acting on behalf of a public official (example: ID badge,

proof of government status, letterhead, memorandum of understanding, purchase order, etc.); and
d) verify in a written statement the legal authority under which the information is requested.

HIPAA
Privacy Rule

Section 164.520 Notice of privacy practices for protected health information.

What you need to know:

1. **The individual's rights**
   An individual (with the except of inmates in a correctional facility) has the right to know:
   a) how you will use or disclose their protected health information;
   b) their rights with respect to protected health information; and
   c) your legal duties with respect to protected health information.

2. **Privacy notice**
   HIPAA mandates certain elements in the Privacy Notice. While they are all included in the Notice in Attachment E of this manual, more detail about these elements may be found in section 164.520(b) of the Rule.

3. **Joint notice**
   If you participate in an organized health care arrangement you may use a joint notice if:
   a) all entities participating in this arrangement agree to abide by the terms of the notice; and
   b) the notice is altered to reflect more than one covered entity; and
   c) the notice specifically describes:
      1) the entities or class of entities to which the joint notice applies;
      2) the service delivery sites to which the joint notice applies; and
      3) that the entities in this arrangement may share protected health information to carry out treatment, payment or health care operations relating to the arrangement.

4. If information use or disclosure is limited or prohibited by other applicable law, this notice must reflect those limitations or prohibitions.

5. **Optional elements of the notice**
   (Note: these optional elements are NOT included in the sample Notice form.)
   You may include in the notice additional, limited uses or disclosures.

6. **Changes to the notice**
   You must promptly revise and distribute this notice whenever a material change occurs. A change may not be implemented prior to the effective date on the notice.

What you need to do:

1. You must provide each client with a copy of a notice about privacy practices. The elements contained in this notice are mandated by HIPAA. (For a sample

copy of this Notice, see Notice of Privacy Practices for Protected Health Information in Attachment E). It must be written in plain language.

2. If you have a direct treatment relationship with an individual you must provide this notice no later than the date of the first service delivery (including service delivered electronically), or in an emergency treatment situation, as soon as reasonably practicable afterwards.

3. You must make an effort to obtain a written acknowledgement of receipt of the notice by the client, or document the efforts to obtain it and the reason(s) it was not obtained. This must be filed in the client's record.

4. You must post this notice at your service delivery site in a prominent location for clients to see.

5. You must have paper copies of this notice available at your place of service for clients to take upon request.

6. If you maintain a web site that provides information about your services or benefits, you must post this notice on your site and make it available electronically.

7. If the individual agrees, you may provide this notice via e-mail. If the e-mail transmission fails, you must provide it in paper format.

8. If you provide the first service to a client electronically, you must provide an electronic version of this notice at the time of request for first service.

9. You must retain copies of all notices for your records.

HIPAA
Privacy Rule

Section 164.522 Rights to request privacy protection for protected health information.

What you need to know:

1. **Use or disclosure restrictions**
An individual has the right to request that you restrict the use or disclosure of their information to carry out treatment, payment or health care operations.
a) YOU DO NOT HAVE TO AGREE TO A RESTRICTION.
b) If you agree to a restriction, you must:
    1) document and file the restriction and your and your client's agreement to this restriction;
    2) abide by it except when the restricted information is needed to provide emergency treatment, the DHSS Secretary needs the information for an investigation into your compliance with HIPAA, or disclosure of restricted information is required by law, for public health activities or for disclosures about victims of abuse, neglect or domestic violence.
    3) if the release of restricted information is necessary to provide emergency treatment to the individual, you must request that the emergency provider does not disclose it further.
c) If you agreed to a restriction you may terminate it if you or the individual requests termination in writing or verbally with subsequent documentation. Termination is only effective for information created or received after the individual has been informed of this termination.

2. **Accommodating a request**
You must accommodate a reasonable request to receive information by alternative means or at alternative locations. (Example: if you want to e-mail a file to your client but he/she does not have a computer, then you must offer an acceptable alternative to e-mail, such as a paper copy that they can pick up or that can be mailed to them.)
a) You may condition your accommodation based on:
    1) when appropriate, information about how payment, if any, will be handled; and
    2) specification of an alternative method or address.
b) The individual does not have to explain to you why such an accommodation is necessary.

What you need to do:

1. If you agree to restrict the use or disclosure of an individual's information, you must:
a) obtain all requests for restriction in writing, and include both your and the individual's signatures on the agreement;
b) file the agreement in the individual's file; and
c) abide by the agreement.

2. If you agreed to a restriction and need to terminate it, you must:
a) document the agreement to terminate the restriction;
b) document how and when you informed the individual and the effective date;
c) continue to abide by the restriction for information created/received before the effective date of termination.

3. You must make reasonable accommodations to comply with an individual's request for information in a specific format (paper or electronic) or location (at your office, via fax, via e-mail, via ground postal service, etc), without asking the individual why such is necessary. You may condition your accommodation based on payment and on obtaining specific information about format or location from the individual.

HIPAA
Privacy Rule

Section 164.524 Access of individuals to protected health information.

What you need to know:

1. For the duration of time that you retain it, an individual has the right to inspect and obtain a copy of their information except for:
   a) psychotherapy notes;
   b) information you expect to use or are using in a civil, criminal or administrative action or proceeding; and
   c) information that cannot be released according to Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a.

2. You must document all information subject to access by individuals, and the title of the person or office responsible for receiving and processing requests for access.

3. **Acting on requests for information**
   a) You may require requests in writing if you have informed your clientele in advance of such a requirement.
   b) Once you have received a request you must act upon it no later than 30 (for information kept on site) or 60 (for information kept at an off-site location) days from receipt by informing the individual of acceptance or providing the individual with a written denial.
   c) You may extend your response time only once by no more than 30 days if you provide the individual with a written statement of the reasons for the delay and the date you will complete the action. This statement must be provided to the individual during the original 30 or 60 day time period.
   d) If you do not maintain the information requested but are aware of where it is maintained, you must inform the individual about where they can direct their request.

4. **Denying access**
   a) You may deny access without providing an opportunity for the individual to review the information:
      1) for psychotherapy notes;
      2) for information you expect to use or are using in a civil, criminal or administrative action or proceeding;
      3) for information that cannot be released according to Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a;
      4) if you are working for or under the direction of a correctional institution and obtaining such copy would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmates, employees or other staff;
      5) if the information was created specifically for research in which the individual is participating, and the individual agreed to a temporary suspension of right of access during the course of research, to be reinstated at the completion of research;

6) if denial of access meets the requirements of the Privacy Act, 5 U.S.C. 522a;
7) if the information was obtained from someone other than a health care provider under promise of confidentiality.

b) You must provide an opportunity for the individual to have the denial reviewed if you base your denial on the grounds that access to the information is likely to endanger the life or physical safety of the individual or another person. For this review you must:
1) designate a licensed health care professional who did not participate in the original decision as reviewer;
2) obtain the reviewer's determination within a reasonable period of time;
3) inform the individual in writing of the reviewer's determination; and
4) take action according to the reviewer's determination.

c) You must provide a timely written denial in plain language that contains:
1) the basis for the denial;
2) the individual's right to a review of the denial if appropriate;
3) a description of how and to whom the individual may complain to your office (including name or title and telephone number), or to the DHHS Secretary.

5. **Permitting access to information in whole or in part**

a) You must allow the individual to inspect or obtain a copy of the requested information in either readable paper form or other format to which you have mutually agreed.

b) You may provide a summary in lieu of providing access to the information if the individual agrees in advance to both the summary and to any fees imposed for the creation of such summary.

c) You must provide access within 30 (for information kept on site) or 60 (for information kept at an off-site location) days from receipt of request.

d) You must make reasonable accommodations to comply with an individual's request for information in a specific format (paper or electronic) or location (at your office, via fax, via e-mail, via ground postal service, etc), without asking the individual why such is necessary. You may condition your accommodation based on payment and on obtaining specific information about format or location from the individual.

e) You may impose reasonable cost-based fees for:
1) copying, including cost of supplies and labor;
2) postage; and
3) preparation of a summary.

What you need to do:

1. Provide prospective clients with an information sheet about your practice, including:

a) a list of the information subject to access, subject to access with review, and not subject to access by individuals;

b) the title of the person responsible for receiving and processing requests for access;

c) your requirement that all requests for access to information be in writing;

d) denial review rights of the individual and a copy of your complaint process;

e) possible costs related copying, postage and summary preparation;

2. Revise your complaint process to include the denial process.

3. Develop form letters for responses to request for access.

4. Maintain documentation of all requests, responses, denial reviews, costs and charges and final disposition or outcome.

5. Read this section so you know how you can or cannot respond to requests for access.

HIPAA
Privacy Rule

Section 164.526 Amendment of protected health information.

What you need to know:

1. **Requests for amendment**
   a) The individual has a right to request you amend their information anytime during the time that you retain their information.
   b) Provided that you inform your clients in advance, you may mandate all requests for amendment be in writing and include the reason to support a requested change.

2. **Acting on requests for amendment**
   a) You must act on the request no later than 60 days after receipt of the request. If you are unable to act within this timeframe, you may extend it only once for 30 more days, provided you give the individual a written statement of the reasons for the delay and the date on which action will occur.
   b) You must document and file the title of the person responsible for receiving and processing requests for amendments.

3. **Denying a request for amendment**
   a) You may deny a request for amendment if:
      1) you (or your agency) did not create the information;
      2) the information is not part of the designated record set (defined as any item, collection or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for you);
      3) the information cannot be accessed by the individual (see 164.524); or
      4) the information is accurate and complete.
   b) Denials, in whole or in part, must be in writing and plain language. This denial must:
      1) include the basis for the denial;
      2) include the individual's right to submit and the process for submitting a written statement disagreeing with the denial and the basis for this disagreement, including any reasonable limitation of statement length;
      3) inform the individual that he/she may ask that their request for amendment and the denial be included in any future disclosures of the protected health information subject to the amendment;
      4) include a description of how the individual may complain to you (including the name or title and telephone number of the person designated to receive complaints for you or your agency) or to the DHHS Secretary
   c) If the individual submits a statement of disagreement, you may prepare a written rebuttal. If you prepare a written rebuttal you must supply the individual with a copy.
   d) You must keep documentation of the request, your denial, the statement of disagreement and your rebuttal.
   e) If the individual submits a statement of disagreement, you must include a copy of the individual's request, the denial, any statement of disagreement and your rebuttal (or a summary of all) in future disclosures.
   f) If the individual does not submit a statement of disagreement, you must include a copy of the individual's request and the denial in future disclosures only if the individual specifically requests it (see #3 [b] [3] above).

4. **Accepting the amendment in whole or in part**
   If you accept the amendment you must:
   a) make the appropriate change to the record;
   b) incorporate the request into the record;
   c) inform the individual in a timely manner that the amendment has been accepted;
   d) obtain the individual's agreement to notify others of the amendment if appropriate;
   e) make reasonable efforts to notify others in a timely manner who:
      1) are identified by the individual has having received the protected health information and needing the amendment;
      2) are your business associates, have received the information and who may have to rely on it to care for the individual.

5. If you are informed of an amendment to an individual's record by another covered entity you must amend the designated record set.

What you need to do:

1. Provide prospective clients with an information sheet about your practice, including**:**
   a) all requests for amendment must be in writing and state the reason supporting the requested change;
   b) the name or title of the person in your office designated to receive and process requests for amendment;
2. Develop a form letter incorporating all the required components of a denial to request for amendment.
3. Incorporate denial to request for amendment in your complaint form.
4. Maintain documentation of all requests, responses, denial reviews, costs and charges and final disposition or outcome.
5. Make sure you understand when you can and when you cannot include the request for amendment and denial in future disclosures of the individual's record.

HIPAA
Privacy Rule

Section 164.528 Accounting of disclosures of protected health information.

What you need to know:

1. **The individual's rights**
An individual has the right to receive an accounting of disclosures of their protected health information that occurred less than or up to six years prior to the date of the accounting request, except for disclosures:
a) to carry out treatment, payment and health care operations;
b) to the individuals themselves;
c) pursuant to an authorization (as provided in Section 164.508);
d) made with the individual present;
e) pursuant to use or disclosures permitted in Section 164.502;
f) for national security or intelligence purposes;
g) to correctional institutions or law enforcement officials (as provided in Section 164.512);
h) as part of a limited data set (as provided in Section 164.514); or
i) that occurred prior to your HIPAA compliance date.

2. **Suspension of the individual's rights**
You must temporarily suspend an individual's rights to receive an accounting if a health oversight agency or law enforcement official provides you with a written statement that such an accounting would likely impede the agency's activities, and the statement specifies the time period for the suspension; if such statement is oral, you must document it and limit the suspension to no longer than 30 days from the date of the oral statement.

3. **Acting on the request for an accounting**
a) You must act on the request no later than 60 days after receipt of the request by providing the accounting requested.
b) You may delay the accounting one time with an extension of 30 days if you provide the individual during the 60 day period with a written statement of reasons why you must delay the accounting, and the date you will provide it.
c) You must provide the first accounting in any 12 month period free of charge. You may impose a reasonable, cost-based fee for each additional accounting request during that same 12 month period, if you have informed the individual in advance of this charge and provide the individual with a chance to withdraw or modify their request.
d) You must document and file all requests for accounting, what the individual receives, and the title of the person responsible for receiving and processing accounting requests.

4. **Accountings must include:**
a) the date of disclosure;
b) the name of the entity or person who received the information and address if known;
c) a brief description of the information disclosed; and
d) a brief statement of the purpose of the disclosure.
(See Attachment I for a sample Accounting of Disclosures form for the client record.)

5. **Accountings for research**
   If the accounting includes disclosure for a particular research purpose for 50 or more individuals, the accounting may also include:
   a) the name of the research activity;
   b) a description in plain language of the research activity, its purpose and individual selection criteria; and
   c) the name, address and telephone number of the research sponsor.

What you need to do:

1. Document all disclosures in each individual's record, so the information is available should someone request an accounting.

2. Create a standard form for responding to accounting requests.

3. Know your HIPAA compliance date.

HIPAA
Privacy Rule

Section 164.530 Administrative requirements.

What you need to know:

1. **Privacy Officer**
   You must designate one person in your office as the Privacy Officer. (See Attachment J.)

2. **Staff training**
   You must train and document the training all members of your workforce on HIPAA Privacy policies and procedures:
   a) no later than your compliance date with HIPAA,
   b) as new members join your workforce,
   c) as workforce members change functions or duties, and
   d) as the policies or procedures change.

3. **Office security**
   You must have appropriate safeguards in place at your facility to protect health information from any intentional or unintentional misuse. (See Office Security Tips in Attachment K.)

4. **Complaints**
   a) You must provide all individuals with a complain process.
   b) You must designate one person who is responsible for receiving complaints.
   c) You must document all complaints, investigations and resolutions.

5. **Sanctions**
   You must impose and document all sanctions against any workforce member who fails to comply with the Privacy policies and procedures.

6. **Mitigation of harmful effects**
   If there has been an accidental disclosure or use of information by a workforce member or by a business associate, you must attempt to mitigate any harmful effects from this disclosure or use. Document all actions.

7. **Intimidating or retaliatory acts**
   You may not intimidate, threaten, coerce or discriminate against any individual who
   a) exercises their rights under these policies and procedures;
   b) complains to you or to the DHHS Secretary about you;
   c) assists in an investigation against you under Part C of Title XI; or
   d) reasonably opposes an act that they believe to be unlawful.

8. **Policies and Procedures**
   a) You must document, implement and inform clientele about your policies and procedures to comply with HIPAA Privacy Standards.
   b) If the law changes you must revise, document and inform your clientele about your policies and procedures accordingly.

c) You must keep all documentation for a minimum of six (6) years from its creation or effective date, whichever is later.

What you need to do:

1. Assign a Privacy Officer, and implement the job description for that person.

2. Train and document all training on HIPAA Privacy Standards:
   a) by April 14, 2003;
   b) as new staff are hired;
   c) as staff change functions; and
   d) as the law and your policies/procedures change.

3. Review the physical security measures you have in your office, and strengthen them if necessary. Document all measures you take to assure physical security.

4. Provide all clients with a copy of your complaint process, and specify who in your office should receive the complaint. Document all complaints, investigations and resolutions.

5. Maintain a HIPAA Privacy Policy and Procedure manual in your office. Keep track of any change in HIPAA law, and change your manual and practices accordingly. You may inform clients of any changes by posting a notice in your waiting room, or by handing them a fact sheet. Document whatever action you take.

6. If you are aware a staff member has violated the HIPAA Privacy Policies or Procedures, you must apply sanctions against them and document it.

7. You must attempt to minimize any harm caused by an accidental disclosure or use by a workforce member or business associate. Document it.

8. Keep all documentation for a minimum of 6 years.

HIPAA
Codes and Transactions Rule

Summary

The "administrative simplification" provisions of HIPAA are intended to improve the efficiency of the national health care system by requiring the standardization of certain transactions transmitted electronically by covered entities.

If you are a covered entity and you transmit any of the following electronically, you must comply with the HIPAA Codes and Transactions Rule, by using standard codes developed by your industry authority. For both mental health and alcohol and substance abuse providers, Substance Abuse and Mental Health Services Administration is the authority.

HIPAA Covered Transactions

- health care claims or encounters
- eligibility for a health plan
- referral certifications or authorizations
- health care claim status
- enrollment and disenrollment in a health plan
- health care payment and remittance advice
- health plan premium payments
- coordination of benefits

The following code sets have been adopted by HIPAA:

- International Classification of Diseases, 9th Edition (ICD-9)
- Current Procedural Terminology, 4th Edition (CPT-4)
- Code on Dental Procedures and Nomenclature (CDT)
- Centers for Medicare and Medicaid Services' Common Procedure Coding System (HCPCS)
- National Drug Codes

If you are a covered entity you are required to integrate these uniform codes into your information technology system. The National Association of State Mental Health Directors, Inc. (NASMHPD) and the National Association of State Alcohol and Drug Abuse Directors (NASADAD) collaborated on developing a more complete procedure and modifier code set for the mental health and alcohol and substance abuse treatment industry. These codes can be downloaded from the SAMHSA web site at www.samhsa.gov/hipaa.

Codes that were developed locally can no longer be used unless they are also in one of the five acceptable code sets listed above.

The compliance date for the Codes and Transactions Rule was October 16, 2002. Entities that filed for an extension of this date by submitting a compliance plan to the federal government must comply by October 16, 2003. Testing is required to begin by April 16, 2003.

HIPAA Privacy Regulation Glossary

Taken from the www.mhccm.org HIPAA toolkit

Act	160.103	the Social Security Act.
ANSI	160.103	the American National Standards Institute.
Business associate:	160.103	Does not include a member of the workforce of a covered entity. a person who on behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, performs, or assists in the performance of: a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or any other function or activity regulated by this subchapter; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. A covered entity participating in an organized health care arrangement that performs a function or activity for or on behalf of such organized health care arrangement, or that provides a service as described above to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. A covered entity may be a business associate of another covered entity.
Compliance date	160.103	the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.
Contrary	160.202	when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means: (1) A covered entity would find it impossible to comply with both the State and federal requirements; or (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.
Correctional institution	164.501	any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.
Covered entity	160.103	• A health plan. • A health care clearinghouse. • A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered functions	164.501	those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.
Data aggregation	164.501	with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities

Designated record set	164.501	(1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
Direct treatment relationship	164.501	a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.
Disclosure	164.501	the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Group health plan	160.103	(also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that: • Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or • Is administered by an entity other than the employer that established and maintains the plan.
HCFA	160.103	Health Care Financing Administration within the Department of Health and Human Services.
Health care	160.103	care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: • Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and • Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health care clearinghouse	160.103	a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions: • Processes or facilitates the processing of health information received

		from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. • Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care operations	164.501	any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates: (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances; (iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and (v) Consistent with the applicable requirements of § 164.514, creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).
Health care provider	160.103	a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information	160.103	any information, whether oral or recorded in any form or medium, that: • Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and • Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer	160.103	(as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.
Health maintenance organization	160.103	(HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.
Health oversight agency	164.501	an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.
Health plan	160.103	an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg- 91(a)(2)). Health plan includes the following, singly or in combination: • A group health plan, as defined in this section. • A health insurance issuer, as defined in this section. • An HMO, as defined in this section. • Part A or Part B of the Medicare program under title XVIII of the Act. • The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq. • An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)). • An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy. • An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. • The health care program for active military personnel under title 10 of the United States Code. • The veterans health care program under 38 U.S.C. chapter 17. • The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)). • The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

		• The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
		• An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
		• The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
		• A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
		• Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).
		
		(2) Health plan excludes:
		• Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and
		• A government-funded program (other than one listed in paragraph (1)(i)- (xvi)of this definition):
		  • Whose principal purpose is other than providing, or paying the cost of, health care; or
		  • Whose principal activity is the direct provision of health care to persons; or the making of grants to fund the direct provision of health care to persons.

HHS	160.103	the Department of Health and Human Services.
Implementation specification	160.103	specific requirements or instructions for implementing a standard.
Indirect treatment relationship	164.501	a relationship between an individual and a health care provider in which: (1) The health care provider delivers health care to the individual based on the orders of another health care provider; and (2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.
Individual	164.501	the person who is the subject of protected health information.
Individually identifiable health information	164.501	information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or

		future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Inmate	164.501	a person incarcerated in or otherwise confined to a correctional institution.
Law enforcement official	164.501	an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) Investigate or conduct an official inquiry into a potential violation of law; or (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing	164.501	to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. (1) Marketing does not include communications that meet the requirements of paragraph (2) of this definition and that are made by a covered entity: (i) For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or (ii) That are tailored to the circumstances of a particular individual and the communications are: (A) Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or (B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care. (2) A communication described in paragraph (1) of this definition is not included in marketing if: (i) The communication is made orally; or (ii) The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.
Modify or modification	160.103	refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.
More stringent	160.202	means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria: (1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is: (i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or (ii) To the individual who is the subject of the individually identifiable health information. (2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting in loco parentis of such minor. (3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information. (4) With respect to the form or substance of an authorization or consent for use or

		disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable. (5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration. (6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.
Organized health care arrangement	164.501	(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider; (2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities: (i) Hold themselves out to the public as participating in a joint arrangement; and (ii) Participate in joint activities that include at least one of the following: (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. (3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan; (4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or (5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.
Payment	164.501	(1) The activities undertaken by: (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

		(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to: (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (A) Name and address; (B) Date of birth; (C) Social security number; (D) Payment history; (E) Account number; and (F) Name and address of the health care provider and/or health plan.
Plan sponsor	164.501	is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).
Protected health information	164.501	individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).
Psychotherapy notes	164.501	notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes

		excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
Public health authority	164.501	an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
Relates to the privacy of individually identifiable health information	160.202	with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.
Required by law	164.501	a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court- ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
Research	164.501	a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
Secretary	160.103	the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
Small health plan	160.103	a health plan with annual receipts of $5 million or less.
Standard	160.103	A rule, condition, or requirement: Describing the following information for products, systems, services or practices: Classification of components. Specification of materials, performance, or operations; or Delineation of procedures; or With respect to the privacy of individually identifiable health information.
Standard setting organization	160.103	(SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.
State	160.103	refers to one of the following: For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan. For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam
State law	160.202	a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.
Trading partner agreement	160.103	an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each

		whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)
Transaction	160.103	the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) Health care claims or equivalent encounter information. (2) Health care payment and remittance advice. (3) Coordination of benefits. (4) Health care claim status. (5) Enrollment and disenrollment in a health plan. (6) Eligibility for a health plan. (7) Health plan premium payments. (8) Referral certification and authorization. (9) First report of injury. (10) Health claims attachments. (11) Other transactions that the Secretary may prescribe by regulation.
Treatment	164.501	the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
Use	164.501	with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
Workforce	160.103	employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

HIPAA

PRIVACY RULE
FINAL RULE (12/28/2000) WITH FINAL MODIFICATIONS (8/14/02)

[Federal Register: December 28, 2000 (Volume 65, Number 250)]
[Rules and Regulations]
[Page 82761-82810]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr28de00-35]
[Modifications in Federal Register, August 14, 2002)

PART 160--GENERAL ADMINISTRATIVE REQUIREMENTS

Authority: § 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d-1329d-8) as added by § 262 of Pub. L. 104-191, 110 Stat. 2021-2031 and § 264 of Pub. L. 104-191 (42 U.S.C. 1320d-2(note)).

Subpart A--General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104-191, and section 264 of Public Law 104-191.

§ 160.102 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5) nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate:

(1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Group health plan (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) Health plan includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(ix) The health care program for active military personnel under title 10 of the United States Code.

(x) The veterans health care program under 38 U.S.C. chapter 17.

(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

(xv) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) Health plan excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Individually Identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer or health care clearinghouse; and

(2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Modify or modification refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:

(i) Classification of components.

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of individually identifiable health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

§ 160.104 Modifications.

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

Subpart B--Preemption of State Law

§ 160.201 Applicability.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104-191.

§ 160.202 Definitions.

For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity would find it impossible to comply with both the State and federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual who is the subject of the individually identifiable health information regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form or substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to record keeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

§ 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

§ 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.

(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

§ 160.205 Duration of effectiveness of exception determinations.

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Subpart C--Compliance and Enforcement

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.302 Definitions.

As used in this subpart, terms defined in § 164.501 of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.

(a) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.306 Complaints to the Secretary.

(a) *Right to file a complaint.* A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.

(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the

Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

(c) *Investigation.* The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

§ 160.308 Compliance reviews.

The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.310 Responsibilities of covered entities.

(a) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(c) *Permit access to information.*

(1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law.

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) *Resolution where noncompliance is indicated.*

(1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates a failure to comply, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.

(b) *Resolution when no violation is found.* If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant in writing.

2. A new Part 164 is added to read as follows:

PART 164 — SECURITY AND PRIVACY

Subpart A — General Provisions

Sec.

Subparts B-D — [Reserved]

Subpart E — Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d-2 and 1320d-4, § 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320(d-2 (note)).

Subpart A--General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act and section 264 of Public Law 104-191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

Subpart B-D--[Reserved]

Subpart E--Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions,:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such

activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop- loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost- management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information, § or a limited data set, and fundraising for the benefit of the covered entity.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to

determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual means the person who is the subject of protected health information.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing means:

(1) to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(ii) For treatment of the individual; or

(iii) For case management or care coordination for the individual or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; and

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(III) Employment records held by a covered entity in its role as employer.

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) *Standard.* A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with §164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §164.502 (b), §164.514 (d), and §164.530 (c) with respect to such otherwise permitted or required use or disclosure.

(iv) Pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by § 164.510; and

(vi) As permitted by and in compliance with this section, 164.512, or 164.514 (e), (f), or (g).

(2) *Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) *Standard: Minimum necessary.*

(1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) *Minimum necessary does not apply.* This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under § 164.508;

(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(v) Uses or disclosures that are required by law, as described by § 164.512(a); and

(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: Uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) *Standard: Uses and disclosures of de-identified protected health information.*

(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: Disclosures to business associates.*

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).

(2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

(g)(1) *Standard: Personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: Adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) *Implementation specification: Unemancipated minors.* If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(ii) Notwithstanding the provision of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered

entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

(B) If, and to the extent prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraphs (g)(3)(i)(A), (B) or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) *Implementation specification: Deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) *Implementation specification: Abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) *Standard: Confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) *Standard: Uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims.*

(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

§ 164.504 Uses and disclosures: Organizational requirements.

(a) *Definitions.* As used in this section:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity i accordance with paragraph (c)(3)(iii) of this section.

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Summary health information means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.

(c)(1) *Implementation specification: Application of other provisions.* In applying a provision of this subpart, other than this section, to a hybrid entity:

(i) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;

(ii) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable; and

(iii) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.

(2) *Implementation specifications: Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:

(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(ii) A component that is described by paragraph (c)(3)(iii) of this section does not use or disclose protected health information that)) it creates or receives from or on behalf of the health care component in a way prohibited by this subpart; and

(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by this subpart.

(3) *Implementation specifications: Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.

(ii) The covered entity has the responsibility for complying with § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j), provided that if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were s separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

(A) Covered functions; or

(B) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

(d)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.

(2) *Implementation specifications: Requirements for designation of an affiliated covered entity.*

(i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.

(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).

(3) *Implementation specifications: Safeguard requirements.* An affiliated covered entity must ensure that:

(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and

(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.

(e)(1) *Standard: Business associate contracts.*

(i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.*

(i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.

(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.*

(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f)(1) *Standard: Requirements for group health plans.*

(i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and discloses of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or had disenrolled from a health insurance issuer or HMO offered by the plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and

(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: Requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may sue or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosures is consistent with other applicable requirements of this subpart.

(b) *Standard: consent for uses and disclosures permitted.*

(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosures of protected health information when an authorization, under §164.508 is required or when another condition must be met for such use or disclosures to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.*

(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being request, the protected health information pertains to such relationship and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: Authorizations for uses and disclosures.*

(1) *Authorization required: General rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: psychotherapy notes.* Notwithstanding any other provision of this subpart, other than transition provisions provided for in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

(b) *Implementation specifications: General requirements.—*

(1) *Valid authorizations.*

(i) A valid authorization is a document that Meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section as applicable.(ii) A valid authorization may contain elements or information in addition to the

elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c), of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) *Compound authorizations*. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such)) ;

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.

(4) *Prohibition on conditioning of authorizations*. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorizationfor the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section;

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party) (5) *Revocation of authorizations*. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) *Documentation*. A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) *Implementation specifications: Core elements and requirements.*

(1) *Core elements.* A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

(iv) A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date.) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorizations, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies;

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section the covered entity can condition treatment, enrollment in the health plan or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) *Plain language requirement*. The authorization must be written in plain language.

(4) *Copy to the individual*. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or the disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: use and disclosure for facility directories.*

(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) *Emergency circumstances.*

(i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) *Standard: uses and disclosures for involvement in the individual's care and notification purposes.*

(1) Permitted uses and disclosures.

(i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2),(3), or (4) of this section, as applicable.

(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person tract on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Use and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by

its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written authorization of the individual as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: Uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: uses and disclosures for public health activities.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA regulated products;

(C) To enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookbac); or

(D) To conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the workplace; or

(*2*) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace- related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or

(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: Disclosures about victims of abuse, neglect or domestic violence.*

(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a

social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(d) *Standard: Uses and disclosures for health oversight activities.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or

services.

(3) *Joint activities or investigations.* Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) *Standard: Disclosures for judicial and administrative proceedings.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(*1*) No objections were filed; or

(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) *Standard: Disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: Pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(*3*) De-identified information could not reasonably be used.

(2) *Permitted disclosures: Limited information for identification and location purposes.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and Rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: Victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: Decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) *Permitted disclosure: Crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) *Permitted disclosure: Reporting crime in emergencies.*

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) *Standard: Uses and disclosures about decedents.*

(1) Coroners and medical examiners. A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) Funeral directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) *Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) *Standard: Uses and disclosures for research purposes.*

(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the

research protocol on the individual's privacy rights and related interests;

(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals. based on at least, the presence of the following elements;

(*1*) An adequate plan to protect the identifiers from improper sue and disclosure;

(*2*) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(*3*) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as r4eqired by law, for authorized oversight of the research study or for other research for which the use or disclosures of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the alteration or waiver;

(C) The research could not practicably be conducted without access to and use of the protected health information;

(E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;

(F) There is an adequate plan to protect the identifiers from improper use and disclosure;

(G) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

(H) There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.

(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or

49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) *Standard: Uses and disclosures to avert a serious threat to health or safety.*

(1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: Uses and disclosures for specialized government functions.*

(1) *Military and veterans activities.*

(i) Armed Forces personnel. A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) Veterans. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) Foreign military personnel. A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations.*

(i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; and

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.*

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) *Standard: Disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) *Standard: de-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) *Implementation specifications: re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) *Standard: minimum necessary requirements.* In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) *Implementation specifications: minimum necessary uses of protected health information.*

(i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) *Implementation specification: Minimum necessary disclosures of protected health information.*

(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: Minimum necessary requests for protected health information.*

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) *Implementation specification: Other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set.* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Devise identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

(3) *Implementation Specification: Permitted purposes for uses and disclosures.*

(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) *Implementation specifications: Data use agreement.*

(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set will use or disclose the protected health information for limited purposes.

(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(*1*) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(*2*) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(*3*) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(*4*) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(*5*) Not identify the information or contact the individuals.

(iii) *Compliance.*

(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(*1*) Discontinued disclosure of protected health information to the recipient; and

(*2*) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

(f)(1) *Standard: Uses and disclosures for fundraising.* A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual; and

(ii) Dates of health care provided to an individual.

(2) *Implementation specifications: Fundraising requirements.*

(i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice;

(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: Verification.*

(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

§ 164.520 Notice of privacy practices for protected health information.

(a) *Standard: notice of privacy practices.*

(1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Exception for group health plans.*

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or (B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) *Implementation specifications: content of notice.*

(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW

YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

(ii) *Uses and disclosures.* The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:

(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;

(B) The covered entity may contact the individual to raise funds for the covered entity; or

(C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) *Optional elements.*

(i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or

disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications:* Provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) *Specific requirements for health plans.*

(i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and

(C) Within 60 days of a material revision to the notice, to individuals then covered by the plan.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) *Provide the notice:*

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgement of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgement and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.*

(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: Joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information

created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.*

(i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) A covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate its agreement to a restriction, if :

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity that agrees to a restriction must document the restriction in accordance with § 164.530(j).

(b)(1) *Standard: Confidential communications requirements.*

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive

communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) *Implementation specifications: Conditions on providing confidential communications.*

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

§ 164.524 Access of individuals to protected health information.

(a) *Standard: Access to protected health information.*

(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of

confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: requests for access and timely action.*

(1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity.*

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.*

(i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

(ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the

protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;

(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

(d) *Implementation specifications: Denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based

on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.526 Amendment of protected health information.

(a) *Standard: Right to amend.*

(1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: requests for amendment and timely action.*

(1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity*

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description

must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.*

(i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.*

(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.506;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;

(iv) Pursuant to an authorization as provided in § 164.508;

(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

(viii) As part of a limited data set in accordance with § 164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: Content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement a copy of a written request for a disclosure under §§164.502(a)(2)(ii) or 164.512, if any.:

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, or pursuant to a single authorization under § 164.508, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with §164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such discourse occurred, or may have occurred, including the date of the last such discourse during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the resear4ch and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of hate individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) *Implementation specifications: Provision of the accounting.*

(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

§ 164.530 Administrative requirements.

(a)(1) *Standard: Personnel designations.*

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) *Implementation specification: Personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

(2) *Implementation specifications: Training.*

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) *Implementation specification: Safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(i) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosures.

(d)(1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: Documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) *Standard: Mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) *Standard: Refraining from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(1) *Individuals.* Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) *Individuals and others.* Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) *Standard: Waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) *Standard: Policies and procedures.* A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure

such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) *Standard: Changes to policies or procedures.*

(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5)of this section.

(3) *Implementation specification: Changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: Changes to privacy practices stated in the notice.*

(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: Changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: Documentation. A covered entity must:*

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) *Standard: Group health plans.*

(1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

§ 164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§164.508 and 164.512(i), , a covered entity may use or disclose protected health information, consistent with paragraph (b) and (c) of this section, pursuant to an authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in §164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or discourse and there is no agreed-to restriction in accordance with §164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§164.508 and 164.512(i), a covered entity may, tot he extent allowed by one of the following permissions, use or disclose, for research, protected health information that it crated or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with §164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either

(1) An authorization other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research; or

(3) A waiver, by an IRB, or informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CRF 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with §164.508 if, after the compliance date, informed consent is sought from an individual participating in the research.

(d) Standard: Effect of prior contracts or other arrangements with business associates. Notwithstanding any other provision of this subpart, a covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to crate, received, or use protected health information on its behalf pursuant to a written contact or other written arrangement with such business associate that does not comply with §§164.502(e) and 164.504(e) consistent with the requirement, and only for such time, set forth in paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.*

(1) *Qualification.* Notwithstanding other sections of this subpart, a covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements of §§164.502(e) and 164.504(e), with respect to a particular

business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to October 15, 2002, such covered entity has entered into and is operating pursuant to a written contact or other written arrangement with a business associate for such business activities or provide services that make the entity a business associate; and

(ii) The contract or other arrangement is not renewed or modified from October 15, 2002, until the compliance date set forth in §164.534.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualifications requirements in paragraph (e) of this section, shall be deemed complaint until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after the compliance date set forth in §164.534; or

(ii) April 14, 2004

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information; held by a business associate.

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than February 26, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable:

(1) Health plans other than small health plans--February 26, 2003.

(2) Small health plans--February 26, 2004.

(c) *Health care clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than February 26, 2003.

Go to Regulation Preamble (summary of comments and responses)

List of Subjects in 45 CFR

Part 160

Electronic transactions, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Reporting and recordkeeping requirements.

Part 162

Administrative practice and procedure, Electronic transactions, Health facilities, Health insurance, Hospitals, Incorporation by reference, Medicare, Medicaid, Reporting and recordkeeping requirements.

For the reasons set forth in the preamble, 45 CFR subtitle A, subchapter C, is added to read as follows:

SUBCHAPTER C- ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A – General Provisions

Sec.

Subpart B – [RESERVED]

Authority: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d - 1320d-8), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)).

Subpart A - General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104-191, and section 264 of Public Law 104-191.

§ 160.102 Applicability.

Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

(a) A health plan.

(b) A health care clearinghouse.

(c) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate means a person who performs a function or activity regulated by this subchapter on behalf of a covered entity, as defined in this section. A *business associate* may be a *covered entity*. *Business associate* excludes a person who is part of the covered entity's workforce as defined in this section.

Compliance date means the date by which a covered entity must comply with a standard, implementation specification, or modification adopted under this subchapter.

Covered entity means one of the following:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income Security Act of 1974 (ERISA)(29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care, as defined in section 2791(a)(2) of the Public Health Service (PHS) Act, 42 U.S.C. 300gg-91(a)(2), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that--

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies furnished to an individual and related to the health of the individual. *Health care* includes the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care; counseling; service; or procedure with respect to the physical or mental condition, or functional status, of an individual or affecting the structure or function of the body.

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

(3) Procurement or banking of blood, sperm, organs, or any other tissue for administration to individuals.

Health care clearinghouse means a public or private entity that does either of the following (Entities, including but not limited to, billing services, repricing companies, community health management information systems or community health information systems, and "value-added" networks and switches are *health care clearinghouses* for purposes of this subchapter if they perform these functions.):

(1) Processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of information into nonstandard format or nonstandard data content for a receiving entity.

Health care provider means a provider of services as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u), a provider of medical or other health services as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that --

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b) of the PHS Act, 42 U.S.C. 300gg-91(b)(2), and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791 of the PHS Act, 42 U.S.C. 300gg-91(b)(3), and used in the definition of *health plan* in this section) means a Federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). *Health plan* includes, when applied to government funded programs, the components of the government agency administering the program. *Health plan* includes the following, singly or in combination:

(1) A group health plan, as defined in this section.

(2) A health insurance issuer, as defined in this section.

(3) An HMO, as defined in this section.

(4) Part A or Part B of the Medicare program under title XVIII of the Act.

(5) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396 et. seq.

(6) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(7) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(8) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(9) The health care program for active military personnel under title 10 of the United States Code.

(10) The veterans health care program under 38 U.S.C. chapter 17.

(11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in 10 U.S.C. 1072(4).

(12) The Indian Health Service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.).

(13) The Federal Employees Health Benefit Program under 5 U.S.C. 8902 et seq.

(14) An approved State child health plan under title XXI of the Act, providing benefits that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397 et. seq.

(15) The Medicare + Choice program under part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(16) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

Implementation specification means the specific instructions for implementing a standard.

Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Secretary means the Secretary of Health and Human Services or any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a prescribed set of rules, conditions, or requirements describing the following information for products, systems, services or practices:

(1) Classification of components.

(2) Specification of materials, performance, or operations.

(3) Delineation of procedures.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For health plans established or regulated by Federal law, *State* has the meaning set forth in the applicable section of the United States Code for each health plan.

(2) For all other purposes, *State* means the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among

other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the exchange of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information exchanges:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation.

Workforce means employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity.

§ 160.104 Modifications.

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard.

(c) The Secretary establishes the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

Subpart B [RESERVED]

PART 162--ADMINISTRATIVE REQUIREMENTS

Subpart A--General Provisions

Sec.

Subparts B - H [RESERVED]

Subpart I - General Provisions for Transactions

Subpart J - Code Sets

Subpart K - Health Care Claims or Equivalent Encounter Information

Subpart L - Eligibility for a Health Plan

Subpart M - Referral Certification and Authorization

Subpart N - Health Care Claim Status

Subpart O - Enrollment and Disenrollment in a Health Plan

Subpart P - Health Care Payment and Remittance Advice

Subpart Q - Health Plan Premium Payments

Subpart R - Coordination of Benefits

Authority: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d - 1320d-8), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)).

Subpart A--General Provisions

§162.100 Applicability.

Covered entities (as defined in §160.103 of this subchapter) must comply with the applicable requirements of this part.

§162.103 Definitions.

For purposes of this part, the following definitions apply:

Code set means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A *code set* includes the codes and the descriptors of the codes.

Code set maintaining organization means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part.

Data condition means the rule that describes the circumstances under which a covered entity must use a particular data element or segment.

Data content means all the data elements and code sets inherent to a transaction, and not related to the format of the transaction. Data elements that are related to the format are not *data content*.

Data element means the smallest named unit of information in a transaction.

Data set means a semantically meaningful unit of information exchanged between two parties to a transaction.

Descriptor means the text defining a code.

Designated standard maintenance organization (DSMO) means an organization designated by the Secretary under §162.910(a).

Direct data entry means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer.

Electronic media means the mode of electronic transmission. It includes the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

Format refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction.

HCPCS stands for the Health [Care Financing Administration] Common Procedure Coding System.

Maintain or *maintenance* refers to activities necessary to support the use of a standard adopted by the Secretary, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification.

Maximum defined data set means all of the required data elements for a particular standard based on a specific implementation specification.

Segment means a group of related data elements in a transaction.

Standard transaction means a transaction that complies with the applicable standard adopted under this part.

Subparts B - H [RESERVED]

Subpart I - General Provisions for Transactions

§162.900 - Compliance dates of the initial implementation of the code sets and transaction standards.

(a) Health care providers. A covered health care provider must comply with the applicable requirements of subparts I through N of this part no later than **[OFR–insert 24 months after the effective date of the final rule in the Federal Register**].

(b) Health plans. A health plan must comply with the applicable requirements of subparts I through R of this part no later than one of the following dates:

(1) Health plans other than small health plans-- **[OFR–insert 24 months after the effective date of the final rule in the Federal Register**].

(2) Small health plans-- **[OFR–insert 36 months after the effective date of the final rule in the Federal Register**].

(c) Health care clearinghouses. A health care clearinghouse must comply with the applicable requirements of subparts I through R of this part no later than **[OFR–insert 24 months after the effective date of the final rule in the Federal Register**].

§162.910 Maintenance of standards and adoption of modifications and new standards.

(a) Designation of DSMOs.

(1) The Secretary may designate as a DSMO an organization that agrees to conduct, to the satisfaction of the Secretary, the following functions:

(i) Maintain standards adopted under this subchapter.

(ii) Receive and process requests for adopting a new standard or modifying an adopted standard.

(2) The Secretary designates a DSMO by notice in the **Federal Register**.

(b) Maintenance of standards. Maintenance of a standard by the appropriate DSMO constitutes maintenance of the standard for purposes of this part, if done in accordance with the processes the Secretary may require.

(c) Process for modification of existing standards and adoption of new standards. The Secretary considers a recommendation for a proposed modification to an existing standard, or a proposed new standard, only if the recommendation is developed through a process that provides for the following:

(1) Open public access.

(2) Coordination with other DSMOs.

(3) An appeals process for each of the following, if dissatisfied with the decision on the request:

(i) The requestor of the proposed modification.

(ii) A DSMO that participated in the review and analysis of the request for the proposed modification, or the proposed new standard.

(4) Expedited process to address content needs identified within the industry, if appropriate.

(5) Submission of the recommendation to the National Committee on Vital and Health Statistics (NCVHS).

§162.915 Trading partner agreements.

A covered entity must not enter into a trading partner agreement that would do any of the following:

(a) Change the definition, data condition, or use of a data element or segment in a standard.

(b) Add any data elements or segments to the maximum defined data set.

(c) Use any code or data elements that are either marked "not used" in the standard's implementation specification or are not in the standard's implementation specification(s).

(d) Change the meaning or intent of the standard's implementation specification(s).

§162.920 Availability of implementation specifications.

(a) Access to implementation specifications. A person or organization may request copies (or access for inspection) of the implementation specifications for a standard described in subparts K through R of this part by identifying the standard by name, number, and version. The implementation specifications are available as follows:

(1) ASC X12N specifications. The implementation specifications for ASC X12N standards may be obtained from the Washington Publishing Company, PMB 161, 5284 Randolph Road, Rockville, MD, 20852-2116; telephone 301-949-9740; and FAX: 301-949-9742. They are also available through the Washington Publishing Company on the Internet at http://www.wpc-edi.com/. The implementation specifications are as follows:

(i) The ASC X12N 837 - Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097, as referenced in §§162.1102 and 162.1802.

(ii) The ASC X12N 837 - Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington

Publishing Company, 004010X098, as referenced in §§162.1102 and 162.1802.

(iii) The ASC X12N 837 - Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096, as referenced in §§162.1102 and 162.1802.

(iv) The ASC X12N 270/271- Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092, as referenced in §162.1202.

(v) The ASC X12N 278 - Health Care Services Review - Request for Review and Response, Version 4010, May 2000, Washington Publishing Company, 004010X094, as referenced in §162.1302.

(vi) The ASC X12N 276/277 Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093, as referenced in §162.1402.

(vii) The ASC X12N 834 - Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095, as referenced in §162.1502.

(viii) The ASC X12N 835 - Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091, as referenced in §162.1602.

(ix) The ASC X12N 820 - Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061, as referenced in §162.1702.

(2) Retail pharmacy specifications. The implementation specifications for all retail pharmacy standards may be obtained from the National Council for Prescription Drug Programs (NCPDP), 4201 North 24th Street, Suite 365, Phoenix, AZ, 85016; telephone 602-957-9105; and FAX 602-955-0749. It may also be obtained through the Internet at http://www.ncpdp.org/. The implementation specifications are as follows:

(i) The Telecommunication Standard Implementation Guide, Version 5 Release 1, September 1999, National Council for Prescription Drug Programs, as referenced in §§162.1102, 162.1202, 162.1602, and 162.1802.

(ii) The Batch Standard Batch Implementation Guide, Version 1 Release 0, February 1, 1996, National Council for Prescription Drug Programs, as referenced in §§162.1102, 162.1202, 162.1602, and 162.1802.

(b) Incorporations by reference. The Director of the Office of the Federal Register approves the implementation specifications described in paragraph (a) of this section for incorporation by reference in subparts K through R of this part in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. A copy of the implementation specifications may be inspected at the Office of the Federal Register, 800 North Capitol Street, NW, Suite 700, Washington, DC.

§162.923 Requirements for covered entities.

(a) General rule. Except as otherwise provided in this part, if a covered entity conducts with another covered entity (or within the same covered entity), using electronic media, a transaction for which the Secretary has adopted a standard under this part, the covered entity must conduct the transaction as a standard transaction.

(b) Exception for direct data entry transactions. A health care provider electing to use direct data entry offered by a health plan to conduct a transaction for which a standard has been adopted under this part must use the applicable data content and data condition requirements of the standard when conducting the transaction. The health care provider is not required to use the format requirements of the standard.

(c) Use of a business associate. A covered entity may use a business associate, including a health care clearinghouse, to conduct a transaction covered by this part. If a covered entity chooses to use a business associate to conduct all or part of a transaction on behalf of the covered entity, the covered entity must require the business associate to do the following:

(1) Comply with all applicable requirements of this part.

(2) Require any agent or subcontractor to comply with all applicable requirements of this part.

§162.925 Additional requirements for health plans.

(a) General rules.

(1) If an entity requests a health plan to conduct a transaction as a standard transaction, the health plan must do so.

(2) A health plan may not delay or reject a transaction, or attempt to adversely affect the other entity or the transaction, because the transaction is a standard transaction.

(3) A health plan may not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan (for example, coordination of benefits information).

(4) A health plan may not offer an incentive for a health care provider to conduct a transaction covered by this part as a transaction described under the exception provided for in §162.923(b).

(5) A health plan that operates as a health care clearinghouse, or requires an entity to use a health care clearinghouse to receive, process, or transmit a standard transaction may not charge fees or costs in excess of the fees or costs for normal telecommunications that the entity incurs when it directly transmits, or receives, a standard transaction to, or from, a health plan.

(b) Coordination of benefits. If a health plan receives a standard transaction and coordinates benefits with another health plan (or another payer), it must store the coordination of benefits data it needs to forward the standard transaction to the other health plan (or other payer).

(c) Code sets. A health plan must meet each of the following requirements:

(1) Accept and promptly process any standard transaction that contains codes that are valid, as provided in subpart J of this part.

(2) Keep code sets for the current billing period and appeals periods still open to processing under the terms of the health plan's coverage.

§162.930 Additional rules for health care clearinghouses.

When acting as a business associate for another covered entity, a health care clearinghouse may perform the following functions:

(a) Receive a standard transaction on behalf of the covered entity and translate it into a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) for transmission to the covered entity.

(b) Receive a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) from the covered entity and translate it into a standard transaction for transmission on behalf of the covered entity.

§162.940 Exceptions from standards to permit testing of proposed modifications.

(a) Requests for an exception. An organization may request an exception from the use of a standard from the Secretary to test a proposed modification to that standard. For each proposed modification, the organization must meet the following requirements:

(1) Comparison to a current standard. Provide a detailed explanation, no more than 10 pages in length, of how the proposed modification would be a significant improvement to the current standard in terms of the following principles:

(i) Improve the efficiency and effectiveness of the health care system by leading to cost reductions for, or improvements in benefits from, electronic health care transactions.

(ii) Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses.

(iii) Be uniform and consistent with the other standards adopted under this part and, as appropriate, with other private and public sector health data standards.

(iv) Have low additional development and implementation costs relative to the benefits of using the standard.

(v) Be supported by an ANSI-accredited SSO or other private or public organization that would maintain the standard over time.

(vi) Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster.

(vii) Be technologically independent of the computer platforms and transmission protocols used in electronic health transactions, unless they are explicitly part of the standard.

(viii) Be precise, unambiguous, and as simple as possible.

(ix) Result in minimum data collection and paperwork burdens on users.

(x) Incorporate flexibility to adapt more easily to changes in the health care infrastructure (such as new services, organizations, and provider types) and information technology.

(2) Specifications for the proposed modification. Provide specifications for the proposed modification, including any additional system requirements.

(3) Testing of the proposed modification. Provide an explanation, no more than 5 pages in length, of how the organization intends to test the standard, including the number and types of health plans and health care providers expected to be involved in the test, geographical areas, and beginning and ending dates of the test.

(4) Trading partner concurrences. Provide written concurrences from trading partners who would agree to participate in the test.

(b) Basis for granting an exception. The Secretary may grant an initial exception, for a period not to exceed 3 years, based on, but not limited to, the following criteria:

(1) An assessment of whether the proposed modification demonstrates a significant improvement to the current standard.

(2) The extent and length of time of the exception.

(3) Consultations with DSMOs.

(c) Secretary's decision on exception. The Secretary makes a decision and notifies the organization requesting the exception whether the request is granted or denied.

(1) Exception granted. If the Secretary grants an exception, the notification includes the following information:

(i) The length of time for which the exception applies.

(ii) The trading partners and geographical areas the Secretary approves for testing.

(iii) Any other conditions for approving the exception.

(2) Exception denied. If the Secretary does not grant an exception, the notification explains the reasons the Secretary considers the proposed modification would not be a significant improvement to the current standard and any other rationale for the denial.

(d) Organization's report on test results. Within 90 days after the test is completed, an organization that receives an exception must submit a report on the results of the test, including a cost-benefit analysis, to a location specified by the Secretary by notice in the **Federal Register**.

(e) Extension allowed. If the report submitted in accordance with paragraph (d) of this section recommends a modification to the standard, the Secretary, on request, may grant an extension to the period granted for the exception.

Subpart J - Code Sets

§162.1000 General requirements.

When conducting a transaction covered by this part, a covered entity must meet the following requirements:

(a) Medical data code sets. Use the applicable medical data code sets described in §162.1002 as specified in the implementation specification adopted under this part that are valid at the time the health care is furnished.

(b) Nonmedical data code sets. Use the nonmedical data code sets as described in the implementation specifications adopted under this part that are valid at the time the transaction is initiated.

§162.1002 Medical data code sets.

The Secretary adopts the following code set maintaining organization’s code sets as the standard medical data code sets:

(a) International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9- CM), Volumes 1 and 2 (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions:

(1) Diseases.

(2) Injuries.

(3) Impairments.

(4) Other health problems and their manifestations.

(5) Causes of injury, disease, impairment, or other health problems.

(b) International Classification of Diseases, 9th Edition, Clinical Modification, Volume 3 Procedures (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

(1) Prevention.

(2) Diagnosis.

(3) Treatment.

(4) Management.

(c) National Drug Codes (NDC), as maintained and distributed by HHS, in collaboration with drug manufacturers, for the following:

(1) Drugs.

(2) Biologics.

(d) Code on Dental Procedures and Nomenclature, as maintained and distributed by the American Dental Association, for dental services.

(e) The combination of Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by HHS, and Current Procedural Terminology, Fourth Edition (CPT-4), as maintained and distributed by the American Medical Association, for physician services and other health care services. These services include, but are not limited to, the following:

(1) Physician services.

(2) Physical and occupational therapy services.

(3) Radiologic procedures.

(4) Clinical laboratory tests.

(5) Other medical diagnostic procedures.

(6) Hearing and vision services.

(7) Transportation services including ambulance.

(f) The Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services. These items include, but are not limited to, the following:

(1) Medical supplies.

(2) Orthotic and prosthetic devices.

(3) Durable medical equipment.

§162.1011 Valid code sets.

Each code set is valid within the dates specified by the organization responsible for maintaining that code set.

Subpart K - Health Care Claims or Equivalent Encounter Information

§162.1101 Health care claims or equivalent encounter information transaction.

The health care claims or equivalent encounter information transaction is the transmission of either of the following:

(a) A request to obtain payment, and the necessary accompanying information from a health care provider to a health plan, for health care.

(b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care.

§162.1102 Standards for health care claims or equivalent encounter information.

The Secretary adopts the following standards for the health care claims or equivalent encounter information transaction:

(a) Retail pharmacy drug claims. The National Council for Prescription Drug Programs (NCPDP) Telecommunication Standard Implementation Guide, Version 5 Release 1, September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1 Release 0, February 1, 1996. The implementation specifications are available at the addresses specified in §162.920(a)(2).

(b) Dental Health Care Claims. The ASC X12N 837 - Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097. The implementation specification is available at the addresses specified in §162.920(a)(1).

(c) Professional Health Care Claims. The ASC X12N 837 - Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098. The implementation specification is available at the addresses specified in §162.920(a)(1).

(d) Institutional Health Care Claims. The ASC X12N 837 - Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096. The implementation specification is available at the addresses specified in §162.920(a)(1).

Subpart L - Eligibility for a Health Plan

§162.1201 Eligibility for a health plan transaction.

The eligibility for a health plan transaction is the transmission of either of the following:

(a) An inquiry from a health care provider to a health plan, or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee:

(1) Eligibility to receive health care under the health plan.

(2) Coverage of health care under the health plan.

(3) Benefits associated with the benefit plan.

(b) A response from a health plan to a health care provider's (or another health plan's) inquiry described in paragraph (a) of this section.

§162.1202 Standards for eligibility for a health plan.

The Secretary adopts the following standards for the eligibility for a health plan transaction:

(a) Retail pharmacy drugs. The NCPDP Telecommunication Standard Implementation Guide, Version 5 Release 1, September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1 Release 0, February 1, 1996. The implementation specifications are available at the addresses specified in §162.920(a)(2).

(b) Dental, professional, and institutional. The ASC X12N 270/271- Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092. The implementation specification is available at the addresses specified in §162.920(a)(1).

Subpart M -Referral Certification and Authorization

§162.1301 Referral certification and authorization transaction.

The referral certification and authorization transaction is any of the following transmissions:

(a) A request for the review of health care to obtain an authorization for the health care.

(b) A request to obtain authorization for referring an individual to another health care provider.

(c) A response to a request described in paragraph (a) or paragraph (b) of this section.

§162.1302 Standard for Referral certification and authorization.

The Secretary adopts the ASC X12N 278 - Health Care Services Review--Request for Review and Response, Version 4010, May 2000, Washington Publishing Company, 004010X094 as the standard for the referral certification and authorization transaction. The implementation specification is available at the addresses specified in §162.920(a)(1).

Subpart N - Health Care Claim Status

§162.1401 Health care claim status transaction.

A health care claim status transaction is the transmission of either of the following:

(a) An inquiry to determine the status of a health care claim.

(b) A response about the status of a health care claim.

§162.1402 Standard for health care claim status.

The Secretary adopts the ASC X12N 276/277 Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093 as the standard for the health care claim status transaction. The implementation specification is available at the addresses specified in §162.920(a)(1).

Subpart O - Enrollment and Disenrollment in a Health Plan

§162.1501 Enrollment and disenrollment in a health plan transaction.

The enrollment and disenrollment in a health plan transaction is the transmission of subscriber enrollment information to a health plan to establish or terminate insurance coverage.

§162.1502 Standard for enrollment and disenrollment in a health plan.

The Secretary adopts the ASC X12N 834 - Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095 as the standard for the enrollment and disenrollment in a health plan transaction. The implementation specification is available at the addresses specified in §162.920(a)(1).

Subpart P -Health Care Payment and Remittance Advice

§162.1601 Health care payment and remittance advice transaction.

The health care payment and remittance advice transaction is the transmission of either of the following for health care:

(a) The transmission of any of the following from a health plan to a health care provider's financial institution:

(1) Payment.

(2) Information about the transfer of funds.

(3) Payment processing information.

(b) The transmission of either of the following from a health plan to a health care provider:

(1) Explanation of benefits.

(2) Remittance advice.

§162.1602 Standards for health care payment and remittance advice.

The Secretary adopts the following standards for the health care payment and remittance advice transaction:

(a) Retail pharmacy drug claims and remittance advice. The NCPDP Telecommunication Standard Implementation Guide, Version 5 Release 1, September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1 Release 0, February 1, 1996. The implementation specifications are available at the addresses specified in §162.920(a)(2).

(b) Dental, professional, and institutional health care claims and remittance advice. The ASC X12N 835 - Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091. The implementation specification is available at the addresses specified in §162.920(a)(1).

Subpart Q - Health Plan Premium Payments

§162.1701 Health plan premium payments transaction.

The health plan premium payment transaction is the transmission of any of the following from the entity that is arranging for the provision of health care or is providing health care coverage payments for an individual to a health plan:

(a) Payment.

(b) Information about the transfer of funds.

(c) Detailed remittance information about individuals for whom premiums are being paid.

(d) Payment processing information to transmit health care premium payments including any of the following:

(1) Payroll deductions.

(2) Other group premium payments.

(3) Associated group premium payment information.

§162.1702 Standard for health plan premium payments.

The Secretary adopts the ASC X12N 820 - Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061 as the standard for the health plan premium payments transaction. The implementation specification is available at the addresses specified in §162.920(a)(1).

Subpart R - Coordination of Benefits

§162.1801 Coordination of benefits transaction.

The coordination of benefits transaction is the transmission from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan, of either of the following for health care:

(a) Claims.

(b) Payment information.

§162.1802 Standards for coordination of benefits.

The Secretary adopts the following standards for the coordination of benefits information transaction:

(a) Retail pharmacy drug claims. The NCPDP Telecommunication Standard Implementation Guide, Version 5 Release 1, September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1 Release 0, February 1, 1996. The implementation specifications are available at the addresses specified in §162.920(a)(2).

(b) Dental claims. The ASC X12N 837 - Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097. The implementation specification is available at the addresses specified in §162.920(a)(1).

(c) Professional health care claims. The ASC X12N 837 - Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098. The implementation specification is available at the addresses specified in §162.920(a)(1).

(d) Institutional health care claims. The ASC X12N 837 - Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096. The implementation specification is available at the addresses specified in §162.920(a)(1).

Authority: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d - 1320d-8), as added by sec. 262 of Public Law 104-191, 110 Stat. 2021-2031, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)).

(Catalog of Federal Domestic Assistance Program No. 93.774, Medicare--Supplementary Medical Insurance Program)

Dated: July 25, 2000

Donna Shalala
Secretary

BILLING CODE 4120-01

Medical Privacy - National Standards to Protect the Privacy of Personal Health Information

SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS

(Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions1

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].

Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].

Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as

a personal representative in accordance with 45 CFR § 164.502(g).

Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]

Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:

[List Purposes].

Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B).

Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices

and Restrictions [provisions dependent on business arrangement]

Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]

Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or

If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

[Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

Effect of Termination.

Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall

retain no copies of the Protected Health Information.

In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.

Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

1 Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

NOTICE OF USE OF PRIVATE HEALTH INFORMATION
Effective Date: April 14, 2003
(form adapted from the Ohio Department of Job and Family Services)

FOR YOUR PROTECTION

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

YOUR HEALTH INFORMATION IS PRIVATE
Keeping your health information private is one of our most important responsibilities. We are committee to protecting your health information and following all laws regarding the use of your health information. The laws say:

1. We must keep your health care information from others who do not need to know it.
2. You may ask that we not share certain health information. (In some instances we may not be able to agree with your request.)

WHO SEES MY HEALTH INFORMATION?
Your private health information may be used by the health care providers (such as substance abuse treatment counselors, mental health providers, doctors, nurses, etc.) who take care of you. We need this information in order to plan your care. When appropriate we may share health information about you in order to help you get the services you need. We may also use your information to contact you about appointment reminders or to tell you about treatment alternatives.

MAY I SEE MY HEALTH INFORMATION?
You may see your health information unless it is the private notes taken by a mental health provider or it is part of a legal case. Most of the time you may receive a copy if you ask. You may be charged an amount to cover copy costs.

If you think some of the information is wrong, you may ask in writing that it be changed or that new information be added. You may ask that the changes or new information be sent to others who have received your health information from us. You may ask for a list of any places where health information has been sent, unless it was sent for treatment, payment, quality review, or to make sure we are following the laws protecting your privacy.

WHAT IF MY HEALTH INFORMATION NEEDS TO GO SOMEWHERE ELSE?
You may be asked to sign an authorization form allowing your health care information to go somewhere else if:

1. Your health care provider needs to send it to other places;
2. You want us to sent it to another health care provider; or
3. You want it sent to another person for you.

The authorization form tells us what, where and to whom the information must be sent. Your authorization is good for six (6) months or until the date you put on the form. You can cancel or limit the amount of information sent at any time by letting us know in writing.

If you are less than 18 years old – your parents or guardians will receive your private health information, **unless by law you are able to consent for your own health care treatment**. If you are, then your private health information will not be shared with parents or guardians unless you

sign an authorization form. You may also ask to have your health information sent to a different person that is helping you with your health care.

COULD MY HEALTH INFORMATION BE RELEASED WITHOUT MY AUTHORIZATION?
When private health information is released without an authorization, it is normally used for Treatment, Payment or Operations (managing the business of a health care provider and reporting to agencies that oversee our business, such as state regulators). The release of health information for this purpose is not tracked and we are not accountable to you for it. Any other release made without your authorization is tracked and accounted. We always report:

1. Contagious diseases, birth defects, and cancer
2. Reactions and problems with medicine
3. Victims of abuse, neglect or domestic violence
4. To the government agency that oversees our business
5. To prevent serious threat to your or others' health and safety
6. Work-related injuries
7. Out of state offenders
8. As required by court order and/or supoena
9. If you commit a crime on the premises

HOW CAN I FIND OUT IF MY HEALTH INFORMATION HAS BEEN RELEASED WITHOUT MY AUTHORIZATION?
To find out if your health information has been released without your authorization for purposes other than Treatment, Payment or Operations, contact _____ at _____ and ask for A Request for Accounting of Disclosures form. Simply fill out the form, attach a copy of your most recent picture ID, and send both to: _____.

MAY I HAVE A COPY OF THIS NOTICE?
This notice is yours. If we change anything in it, you will get a new notice. You can obtain additional copies of this notice by asking your health care provider.

QUESTIONS OR COMPLAINTS?
If you have questions about this notice or you think that we have not protected your private health information and you wish to complain about it, please contact:

You can also complain to the Federal Government by writing to the:

Office for Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F, HHH Building
Washington, D.C. 20201-0004
Or by calling the Office for Civil Rights at (800) 368-1019

DATA USE AGREEMENT FOR USE OF (name of agency that is the source of the data) DATA CONTAINING INDIVIDUAL-SPECIFIC INFORMATION) **(form adapted from the Centers for Medicare and Medicaid Services Data Use Agreement, 2001)**

In order to secure **data** that resides in name of the agency that is the source of the data, and in order to ensure the integrity, security, and confidentiality of information maintained by this agency, and to permit appropriate disclosure and **use** of such **data** as permitted by law, name of agency that is the source of the data and _____ enter into this **agreement** to comply with the following specific paragraphs.

1. This **Agreement** is by and between the name of agency that is the source of the data, hereinafter termed "Data Source " and _____ _____, hereinafter termed "User."

2. This **Agreement** addresses the conditions under which Data Source will disclose and the User will obtain and **use** specific **data** file(s) specified in section 7. This **Agreement** supersedes any and all agreements between the parties with respect to the **use** of **data** from the files specified in section 7. Further, the terms of this **Agreement** can be changed only by a written modification to this **Agreement** or by the parties adopting a new **agreement**. The parties agree further that instructions or interpretations issued to the User concerning this **Agreement** or the **data** specified herein, shall not be valid unless issued in writing by the Data Source point-of-contact specified in section 5.

3. The parties mutually agree that Data Source retains all ownership rights to the **data** file(s) referred to in this **Agreement**, and that the User does not obtain any right, title, or interest in any of the **data** furnished by Data Source .

4. The parties mutually agree that the following named individual is designated as Custodian of the file(s) on behalf of the User and the person will be responsible for the observance of all conditions of **use** and for establishment and maintenance of security arrangements as specified in this **Agreement** to prevent unauthorized **use**. The User agrees to notify the Data Source within fifteen (15) days of any change of custodianship. The parties mutually agree that the Data Source may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

_____
(Name of Custodian)

_____
(Company/Organization)

_____
(Street Address)

_____
(City/State/ZIP Code)

_____
(Phone No. - Including Area Code and E-Mail Address, If Applicable)

5. The parties mutually agree that the following named individual will be designated as point-of-contact for the **Agreement** on behalf of the Data Source

_____
(Name of Contact)

_____

(Title/Component)

_____

(Street Address)

_____

(Mail Stop)

_____

(City/State/ZIP Code)

_____

(Phone No. - Including Area Code and E-Mail Address, If Applicable)

6. The User represents, and in furnishing the **data** file(s) specified in section 7 relies upon such representation, that such **data** file(s) will be used solely for the following purpose(s).

_____

_____

_____

The User represents further that the facts and statements made in any study or research protocol or project plan submitted to the Data Source for each purpose are complete and accurate. Further, the User represents that said study protocol(s) or project plans, as have been approved by the Data Source or other appropriate entity as the Data Source may determine, represent the total **use**(s) to which the **data** file(s) specified in section 7 will be put. The User represents further that, except as specified in an Attachment to this **Agreement** or except as the Data Source shall authorize in writing, the User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the **data** covered by this **Agreement** to any person. The User agrees that, within the User organization, access to the **data** covered by this **Agreement** shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this section and to those individuals on a need-to-know basis only. The User also:

7. The following **data** file(s) is/are covered under this **Agreement**.
File /Year(s)

_____

_____

8. The parties mutually agree that the aforesaid file(s) (and/or any derivative file(s) [includes any file that maintains or continues identification of individuals]) may be retained by the User until, hereinafter known as the "retention date." The User agrees to notify the Data Source within 30 days of the completion of the purpose specified in section 6 if the purpose is completed before the aforementioned retention date. Upon such notice or retention date, whichever occurs sooner, the Data Source will notify the User either to return all **data** files to the Data Source at the User's expense or to destroy such **data**. If the Data Source elects to have the User destroy the **data**, the User agrees to certify the destruction of the files in writing within 30 days of receiving the Data Source's instruction. A statement certifying this action must be sent to the Data Source. If the Data Source elects to have the **data** returned, the User agrees to return all files to the Data Source within 30 days of receiving notice to that effect. The User agrees that no **data** from the Data Source records, or any parts thereof, shall be retained when the aforementioned file(s) are returned or destroyed unless authorization in writing for the retention of such file(s) has been received from the appropriate Systems Manager. The User acknowledges that stringent adherence to the aforementioned retention date is required, and that the User shall ask the Data Source for instructions under this paragraph if instructions have not been received after 30 days after the retention date.

The **Agreement** may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, the Data Source will cease releasing **data** to the User under this **Agreement** and will notify the User either to return all previously released **data** files to the Data Source at the User's expense or destroy such **data**, using the same procedures stated in the above paragraph of this section. Sections 3, 6, 8, 11, 12, 13, 14, 16, 17 and 18 shall survive termination of this **Agreement**.

9. The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the **data** and to prevent unauthorized **use** or access to it. The User acknowledges that the **use** of unsecured telecommunications, including the Internet, to transmit individually identifiable or deducible information derived from the file(s) specified in section 7 is prohibited. Further, the User agrees that the **data** must not be physically moved or transmitted in any way from the site indicated in item number 4 without written approval from the Data Source .

10. The User agrees that the authorized representatives of the Data Source will be granted access to premises where the aforesaid file(s) are kept for the purpose of inspecting security arrangements confirming whether the User is in compliance with the security requirements specified in paragraph 9.

11. The User agrees that no findings, listing, or information derived from the file(s) specified in section 7, with or without identifiers, may be released if such findings, listing, or information contain any combination of **data** elements that might allow the deduction of a beneficiary's identification without first obtaining written authorization from the appropriate System Manager. Examples of such **data** elements include but are not limited to geographic indicator, age, sex, diagnosis, procedure, admission/discharge date(s), or date of death. The User agrees further that the Data Source shall be the sole judge as to whether any finding, listing, information, or any combination of **data** extracted or derived from the Data Source's files identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual to a reasonable degree of certainty.

12. The User agrees that the User shall make no attempt to link records included in the file(s) specified in section 7 to any other identifiable source of information. This includes attempts to link to other the Data Source **data** file(s). The inclusion of linkage of specific files in a study protocol approved in accordance with section 6 is considered express written authorization from the Data Source .

13. The User agrees to submit to the Data Source a copy of all findings within 30 days of making such findings. The parties mutually agree that the User has made findings with respect to the **data** covered by this **Agreement** when the User prepares any report or other writing for submission to any third party (including but not limited to any manuscript to be submitted for publication) concerning any purpose specified in section 6 (regardless of whether the report or other writing expressly refers to such purpose, to the Data Source , or to the files specified in section 7 or any **data** derived from such files).

14. The User understands and agrees that they may not reuse original or derivative **data** file(s) without prior written approval from the appropriate System Manager.

15. The parties mutually agree that the following specified Attachments are part of this **Agreement**: _____

16. On behalf of the User the undersigned individual hereby attests that he or she is authorized to enter into this **Agreement** and agrees to all the terms specified herein.

_____
(Name and Title of Individual - Typed or Printed)

_____
(Company/Organization)

_____
(Street Address)

_____
(City/State/ZIP Code)

_____
(Phone No. - Including Area Code and E-Mail Address, If Applicable)

_____
(Signature)
(Date)

17. The Custodian, as named in paragraph 4, hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User, and agrees to comply with all of the provisions of this **Agreement** on behalf of the User.

_____
(Typed or Printed Name and Title of Custodian of File(s)

_____
(Signature) (Date)

18. On behalf of the Data Source the undersigned individual hereby attests that he or she is authorized to enter into this **Agreement** and agrees to all the terms specified herein.

_____
(Typed or Printed Name and Title of the Data Source Representative)

_____
(Signature) (Date)

AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

1. Name: _____
   Last Name First Name Middle Initial

2. Date of Birth: _____/_____/_____ 3. Date of Admission/Discharge: _____/____/____
   Month/ Day / Year Month Day Year

4. Date authorization initiated: _____/_____/_____
   Month Day Year

5. Authorization initiated by: _____
   Name of Individual Relationship to client or provider

6. Description of the information to be used or disclosed, and purpose for each. Be specific.

Description of information	Purpose of use or disclosure
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

(use another sheet if more lines are required)

(Client may state, "at my request" for "purpose" when the client initiates the authorization but elects not to provide a statement of purpose.)

7. Name of the person or classes of persons authorized to make such a use or disclosure:
_____

8. Name of the person or classes of persons to whom you may make the requested use or disclosure: _____

9. Expiration date or event upon which this authorization is no longer valid and this information can no longer be used or disclosed as specified in this authorization:
_____
(For the authorization is to be used specifically for research, "end of the research study" or "none" is sufficient for expiration date.)

10. Signature of the client or personal representative: _____

11. Date of signature: _____/_____/_____
    Month Day Year

12. (If a personal representative was used, describe the client's personal representative's authority to act: _____)

The following specifies your rights about this authorization under the Health Insurance Portability and Accountability Act (HIPAA).

1. Tell your counselor if you don't understand this form, and the counselor will explain it to you.

2. You have the right to revoke or cancel this authorization at any time, EXCEPT:
   - A. to the extent information has already been shared based on this authorization; or
   - B. the authorization was obtained as a condition of obtaining insurance coverage.

   To revoke or cancel this authorization you must submit your request in writing to this agency.

3. You may be required to complete this authorization before receiving treatment if:
   - A. you are in a research-related treatment program and the information will be used specifically for that research;
   - B. you have authorized your treatment provider to disclose information about you to a third party (another treatment provider, an insurance or health plan, etc.), unless the information provided is psychotherapy notes; or
   - C. you are receiving psychotherapy services.

4. If you refuse to sign this authorization, and you are in a research-related treatment program or have authorized your provider to disclose information about you to a third party, your provider has the right to decide not to treat you or accept you as a client in their practice.

5. Once the information about you leaves this office according to the terms of this authorization, this office or agency has no control over how it will be used by the recipient. You need to be aware that at that point your information may no longer be protected by HIPAA.

6. If this agency initiated this authorization form, you must receive a copy of the signed authorization.

(You may combine this with the HIPAA authorization or keep them separate.)

Consent Form for the Release of Confidential Alcohol and Substance Abuse Treatment Services Information

I, _____, authorize _____
Name of Patient — Name of alcohol/drug program making disclosure

to disclose to _____ the following information:
Name of person or organization to which disclosure is to be made

_____
(Nature and amount of information to be disclosed, as limited as possible)

The purpose of the disclosure authorized in this consent is to:

_____
(Purpose of disclosure, as specific as possible)

I understand that my alcohol and/or drug treatment records are protected under the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2, and cannot be disclosed without my written consent unless otherwise provided for in the regulations. I also understand that I may revoke this consent at any time except to the extent that action has been taken in reliance on it, and that in any event this consent expires automatically as follows:

_____
(Specify the date, event or condition upon which this consent expires)

Dated: _____/_____/_____
Month / Day / Year

Signature of Patient: _____

_____
Signature of parent, guardian or authorized representative When required

Information Flow Assessment Questionnaire

Instructions:
1. Check off your name

___ (Other – be specific: _____)

2. There are eight sections to this questionnaire: A. Information Created, Received, Sent and/or Stored; B. Access to Health Information; C. Health Information Sources; D. Information Transmission; E. Disposal Methods; F. Business Associate List; G. Additional Information; and H. Storage List. Complete sections A through G. Section H is for reference only.

SECTION – A. INFORMATION CREATED, RECEIVED, SENT AND/OR STORED

1. Identify those items that contain client health information that you current create, receive, send and/or store in your work and in your work area.
"Client health information" is defined as any info created or received by a provider or contractor that identifies or could be used to identify an individual client.
"Client identifiers" include any or all of the following: name, date of birth, all ages >89, address, city, county, judicial district, admission or discharge date, telephone or fax numbers, e-mail address, SSN, medical record number, vehicle identifiers, photos or date of death.

2. Check all options that apply for each column and each category. If a description is not listed, add it to the appropriate category.

3. To complete the Storage Information column, use one or all of the following as appropriate:
Under the **Type** column, use **O** for original and **C** for copy
Under the **Format** column, use **P** for paper and **E** for electronic
Under the **How Stored** column, use the Storage List (Section G, page 18) to obtain the appropriate number(s).

"Storage" is defined as client health information retained in your work area for more than 30 days.

ADMINISTRATIVE **STORAGE**

Information Description	Create	Receive	Send	Store	Type	Format	How Stored	Work on Info but Store Elsewhere (Specify)
					O C	P E	Use List	
Complaints								
Critical Incidents								
Correspondence, Memos (internal & external)								
Investigations								
Legal issues								
Contract Monitoring								
Meetings, Minutes/Notes								
Questionnaires								

Inquiries about services								
Photographs								
Site Visits								
Background checks								
Community relations								
None (go to next section)								

FISCAL **STORAGE**

Information Description	**Create**	**Receive**	**Send**	**Store**	**Type**	**Format**	**How Stored**	**Work on Info but Store Elsewhere (Specify)**
					O C	**P E**	**Use List**	
Billing/Remittance Advices								
Claims Information								
Contracts								
Correspondence								
Funding Justifications								
Questionnaires, Forms								
Medicaid								
Contract Monitoring								
Site Visits								
Reports								
Banking/Direct Deposit								
Meeting Minutes/notes								
None (go to next section)								

TREATMENT **STORAGE**

Information Description	**Create**	**Receive**	**Send**	**Store**	**Type**	**Format**	**How Stored**	**Work on Info but Store Elsewhere (Specify)**

					O C	P E	Use List	
Contract monitoring								
Site visits								
Complaints/critical incidents								
Licensing								
Inquiries about services								
Training								
Correspondence								
Meetings								
Contracting								
Case consultations								
Logs or registries								
Quality assurance/improvement								
Referrals								
Laboratory data								
Commitments								
Reporting								
None (go to next section)								

CLINICAL TREATMENT PROVIDERS **STORAGE**

Information Description	Create	Receive	Send	Store	Type	Format	How Stored	Work on Info but Store Elsewhere (Specify)
					O C	P E	Use List	
Assessments/tests/reports								
History								
Treatment plan								
Laboratory data								
Medication								
Progress notes								
Case management								
Admission/Discharge summaries								
Referrals								
Transfers								
Training								

Volunteers								
Students/internships								
Contractors								
Phone call documentation								
Follow-up post discharge care								
Waiting list								
Data collection instruments (DACODS, DRS)								
Client records/files								
Complaints/critical incidents								
Legal issues								
Meetings								
Clinical supervision								
Family involvement								
Commitments								
Reporting								
Abuse reporting								
Medical/psychological consults								
None (go to next section)								

PREVENTION

STORAGE

Information Description	**Create**	**Receive**	**Send**	**Store**	**Type**	**Format**	**How Stored**	**Work on Info but Store Elsewhere (Specify)**
					O C	**P E**	**Use List**	
Contracting								
Contract monitoring								
Education/training classes								
School interventions								
Community relations								
Reporting								

None (go to next section)								

PREVENTION PROVIDERS **STORAGE**

Information Description	Create	Receive	Send	Store	Type		Format		How Stored	Work on Info but Store Elsewhere (Specify)
					O	C	P	E	Use List	
Contracting										
Contract monitoring										
Education/training classes										
School interventions										
Community relations										
None (go to next section)										

DATA **STORAGE**

Information Description	Create	Receive	Send	Store	Type		Format		How Stored	Work on Info but Store Elsewhere (Specify)
					O	C	P	E	Use List	
Data										
Reports										
Site Visits										
Contract monitoring										
Phone call documentation										
None (go to next section)										

Information Description	**Create**	**Receive**	**Send**	**Store**	**Type**	**Format**	**How Stored**	**Work on Info but Store Elsewhere (Specify)**
					O C	**P E**	**Use List**	

Information Description	**Create**	**Receive**	**Send**	**Store**	**Type**	**Format**	**How Stored**	**Work on Info but Store Elsewhere (Specify)**
					O C	**P E**	**Use List**	

TRANSACTIONS

For the transactions listed below, specify whether health information is created, sent, received, or stored electronically (**E**), on paper (**P**), and/or by Voice (**V**). Voice includes face-to-face, phone or voicemail. Select all that apply.

Description	**Create**	**Receive**	**Send**	**Store**
	E P V	**E P V**	**E P V**	**E P V**
Authorization for services				
Consent for services				
Coordination of benefits				
Eligibility information				
Enrollment/disenrollment in health plan				

Bill or claim				
Billing or claim status				
Payment and remittance advice				
Claims attachments				
Premium payments				
None (go to next section)				

DIAGNOSIS/PROCEDURE CODES

Specify your source for diagnosis/procedure codes in the following table by checking the appropriate box on the right.

Reference	**Specify (Ö)**
DSM-III (American Psychiatric Association, “Diagnostic and Statistical Manual of Mental Disorders” third edition)	
DSM-IV (American Psychiatric Association, “Diagnostic and Statistical Manual of Mental Disorders” fourth edition	
ICD-9CM (International Classification of Diseases, 9th edition)	
ICD-10CM (International Classification of Diseases, 10th edition)	
CPT (AMA, “Current Procedural Terminology Coding, Fourth edition)	
HCPCS (HCFA/CMS “Common Procedure Coding System”)	
HCPCS J-Codes (HCPCS Pharmacy Codes)	
Local Codes (W and Y codes)	
NDC (HHS, “National Drug Codes”)	
DRGs (“Diagnostic Related Groupings”)	
None (go to next section)	

ELECTRONIC SYSTEMS

Select the current system(s)/application you use. For each system selected, indicate if the system can be accessible from an area other than the worksite, and if so, how the system is accessed. If a system you use is not listed, write it in. If a mode of access you use is not listed, write it in the **Other** column.

System/Application	**Use**	**Remote Access**		**Access Mode**					
		Yes	**No**	**PC**	**E-mail**	**Disk**	**Web**	**Data line**	**Other**
Treatment Management System									

DACODS			
DRS			
Fiscal			
TEDS			
ADDSCODS			
Methadone Registry			
IC Database			
Special Connections Database			
COFRS			
Medicaid			
Prevention			
Minimum Data Set			
Stories			
None (go to next section)			

SECTION - B. ACCESS TO HEALTH INFORMATION

BUILDING

Identify the names of those persons who have access to your work area's physical location and to the health information you maintain. Specify their type of access by writing a **U** for Unlimited or **L** for Limited in the Access columns. If the category of person is not listed, write it in.

Who	Names	Access	
		Within Bldg.	Within Work Areas

Clients			
Contractors			
Employees (non-ADAD)			
General Public			
Family/friends, etc.			
Professionals (Attorneys/Auditors)			
Volunteers			
Training/Internship			
Other			
None (go to next section)			

LOCATION

Identify all the physical site(s) where health information may be located in your work area. Specify with a check mark by the appropriate options.

Storage Mechanism	**Hallway**	**Unsecured Common Work Area**	**Secured Work Area**	**Shared Work Area**	**Private Work Area**	**File/Storage Room**	**Other**
Computer							
Copier							
Fax							

File/Storage Cabinets							
Off-site (Home, Car, Briefcase)							
Open Shelves/Bookcase							
Printer							
Recycle Container							
Shredder							
None (go to next section)							

ACCESS CONTROL

Identify access controls that are in place for protecting health information maintained in your work area. Select all that apply by checking the appropriate box.

Current Access Control	**Check (Ö)**
Identification	
Badges/ID	
Optical Recognition	
Fingerprint	
Passwords	
Staff Escort	
Visual Recognition	
Observation	
Employee monitored areas	
On-site Security Force	

24 hr. Surveillance (camera, motion, heat)	
Afterhours Surveillance (alarms, monitors)	
Reception Area	
Receptionist/Guard/Information	
Sign-in/out Register (Monitored)	
Sign-in/out Register (Unmonitored)	
Physical Barriers	
Counter/Desk/Table	
Doors	
Open	
Closed (unlocked)	
Locked – card swipe	
Locked – combination/key pad	
Locked – keys	
Partitions/Moveable dividers	
Glass	
Wall	
Hours	
Closed (Open by Request Only)	
Open 24 hours 7 days/week	
Open Days (Mon. through Fri.)	
Open Days (Mon. through Sat.)	
Open Evenings & Weekends only	
Open Evenings only	
Open variable hours/days	
Other	
Other	

None (go to next section)	

SECTION – C. HEALTH INFORMATION SOURCES

Identify agencies/source(s) to whom or from whom you send or receive health information. Identify whether such transmissions are on paper, electronic, fax or phone by checking the appropriate box. Check all that apply.

Sources	**Send**	**Receive**		**Paper**	**Electronic**	**Fax**	**Phone**	**Other**
Facilities								
Day Treatment								
Residential Treatment								
Outpatient Treatment								
Halfway Houses								
Medically managed non-detox								
Medically managed detox								
Residential detox								
ORT clinics/dispensaries								
DUI education/treatment providers								
Offender facilities								
Medical/psych hospitals								
Nursing Homes								
Rehabilitation centers								
VA hospitals								
MR centers								
Special care centers								
Schools								
Sheltered workshops								
Urgent care centers								
Motor Vehicles								
Managed Service Organization								

Social Services								
Child/Adult Protection Services								
Dept. of Soc. Serv.								
Foster home								
Private Practice								
Attorney								
Chiropractor								
Dentist								
Health Plan/Insurance								
Physician								
Private Allied Health Specialist (Social Worker, Nutritionist)								
Psychologist								
Therapist (Occup, Speech, Phys.,)								
Law Enforcement								
Attorney General's Office								
Clerk of Court								
Court								
District Attorney								
Law Enforcement Officer								
Jail/Detention center								
Parole/Probation								
Prison/correctional facility								
Court evaluator								

Financial								
Auditor								
Bank								
Billing/Collections								
Court								
Estate								
Payer/Insurance Company								
Additional								
Clearinghouse								
Client								
Contractor								
Coroner								
Dept/Div/Public Info Officer								
Employees								
Employers								
Family/Guardian								
Friend/Neighbor								
Legislator (State or Federal)								
Media								
Other state agencies								
Out-of-state agencies								
Researchers/research facility								
Review/Oversight boards								
Transport/Ambulance providers								
Vendors								

None (go to next section)								

SECTION – D. INFORMATION TRANSMISSION

Identify all methods of transmission you use for sending or receiving health information. Also indicate by a check mark if you retain a copy of the information.

Transmission Method	**Send**	**Receive**	**Retain**
Electronic			
File Transfer Protocol (FTP)			
E-mail			
Disk/CD			
LAN or network			
Modem			
Scanner			
Web			
Software application system			
Paper			
Courier/Fed Ex/UPS/Airborne/Emory/etc.			
Sealed envelope/folder			
Unsealed envelope/folder			
FAX			
Hand delivery (person to person)			
Logs/Journals			
Interoffice mail			
US Postal mail			
Client record file			
Voice/Visual			
Face to face			
Pager			
Phone - Cell/Satellite			

Phone – Land line			
Photos			
Security Camera/Tapes			
Tape (reel to reel/cartridge)			
Video tapes			
Web cam			
None (go to next section)			

Identify all methods you use to record health information received verbally.

Recording Method	**Check (Ö)**
Dictate to machine, computer, person	
Enter into PC	
Message/memo	
Note in Logs/Journals	
Informal Staff notes	
Client Record form	
Scratch Pad/Post-It Note	
Tape Cassette/CD	
Message Center	
Voice Mail	
None (go to next section)	

SECTION – E. DISPOSAL METHODS

Identify how you dispose of health information used/maintained in your work area. Check all that apply.

Disposal Method	Check (ö)
Delete/Empty electronic trash	
Send to Permanent storage	
Recycle container	
Personally shred	
Place in box for later shredding	
Throw in trash	
None (go to next section)	

SECTION – F. BUSINESS ASSOCIATE LIST

List out all persons, businesses, organizations or groups to whom you send or share client-identified health information.

Who	Why info is shared

SECTION – G. ADDITIONAL INFORMATION

Write any comments, concerns and/or additional information you may have about confidentiality and protection of health information.

SECTION – H. STORAGE LIST

Use this list when completing Section A – Information Created, Received, Sent and/or Stored. Each method or place of storage is numbered. When completing Section A write-in the number(s) that correspond to the method/location of storage. Add other storage methods if they are not listed by continuing with the numbering sequence.

How Stored	#
Bookshelf/Open shelf files	1
Sealed Boxes	2
Unsealed boxes	3
Bulletin Board	4
Cassette Tape, locked area	5
Cassette Tape, unlocked area	6
Closet/Room/Storage area – locked	7
Closet/Room/Storage area – unlocked	8
Contractors	9
Desk Drawer – locked	10
Desk Drawer – unlocked	11
Desk/Table top	12
Disks/CDs – locked area	13
Disks/CDs – unlocked area	14
E-mail – Network	15

E-mail – PC	16
Envelopes – sealed	17
Envelopes – unsealed	18
File cabinet – locked	19
File cabinet – unlocked	20
Folders – Electronic	21
Folders – Paper	22
Magnetic Tape/Data Cartridge	23
Mailboxes, In/Out	24
Mainframe	25
Microfilm/microfiche	26
Network archival storage	27
Network backups	28
Network server	29
Network, personal drive	30
Network, shared drive	31
Notebooks	32
Off-site Electronic storage	33
Off-site Paper storage	34
PC – C drive	35
PC – H drive	36
PC – shared drive (I, O, etc.)	37
Portable Cart	38
State Records center	39
Vault	40
Voice Mail	41
	42
	43
	44
	45
	46
	47
	48

HIPAA
FORM FOR AN ACCOUNTING OF DISCLOSURES

SAMPLE

Keep the original of this form in the client record and update it each time information about the client is shared with someone outside this office/agency. When the client asks for an accounting of disclosures, copy this form and give them the copy.

Client Name: _____
Last First Middle Initial

Client Date of Birth: _____
Month / Day / Year

Disclosures of Protected Health Information about this Client:

Date of Disclosure	Name of Recipient	Address of Recipient	Information Disclosed	Purpose of Disclosure

Sample (Chief) Privacy Officer Job Description

This document was created from the American Health Information Management Association (AHIMA) Web site (http://www.ahima.org/infocenter/models/privacyofficer2001.htm) and is provided here for your convenience.

Position Title: (Chief) Privacy Officer[1]

Immediate Supervisor: Chief Executive Officer, Senior Executive, or Health Information Management (HIM) Department Head[2]

General Purpose: The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of; and adherence to the organization's policies and procedures covering the privacy of; and access to, patient health information in compliance with federal and state laws and the healthcare organization's information privacy practices.

Responsibilities:

- Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management and administration, the Privacy Oversight Committee,[3] and legal counsel.

- Works with organization senior management and corporate compliance officer to establish an organization-wide Privacy Oversight Committee.

- Serves in a leadership role for the Privacy Oversight Committee's activities.

- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.

- Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

- Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties

- Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.

- Establishes with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity.

- Works cooperatively with the HIM Director and other applicable organization units in

overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.

- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.

- Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.

- Serves as a member of; or liaison to, the organization's IRB or Privacy Committee,[4] should one exist. Also serves as the information privacy liaison for users of clinical and administrative systems.

- Reviews all system-related information security plans throughout the organization'

- s network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.

- Works with all organization personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements

- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.

- Serves as information privacy consultant to the organization for all departments and appropriate entities.

- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.

- Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

Qualifications:

- Certification as an RHIA or RHIT with education and experience relative to the size and scope of the organization.

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Knowledge in and the ability to apply the principles of HIM, project management, and change management.
- Demonstrated organization, facilitation) communication, and presentation skills.
- This description is intended to serve as a scalable framework for organizations in development of a position description for the privacy officer.

Notes

1. The title for this position will vary from organization to organization, and may not be the primary title of the individual serving in the position. “Chief” would most likely refer to very large integrated delivery systems. The term “privacy officer” is specifically mention in the HIPAA Privacy Regulation.

2. Again, the supervisor for this position will vary depending on the institution and its size. Since many of the functions are already inherent in the Health Information or Medical Records Department or function, many organizations may elect to keep this function in that department.

3. The “Privacy Oversight Committee” described here is a recommendation of AHIMA, and should not be considered the same as the “Privacy Committee” described in the HIPAA privacy regulation. A privacy oversight committee could include representation from the organization’s senior administration, in addition to departments and individuals who can lend an organization-wide perspective to privacy implementation and compliance.

4. Not all organizations will have an Institutional Review Board (IRB) or Privacy Committee for oversight of research activities. However, should such bodies be present or require establishment under HJPAA or other federal or state requirements, the privacy officer will need to work with this group(s) to ensure authorizations and awareness are established where needed or required.

OFFICE SECURITY TIPS - SECURING YOUR WORK AREA

1. If you leave papers with client identifiers on your desk, turn them print side down.
2. Don't throw away any papers with client identifiers. Shred them.
3. Clear protected health information from your computer screen before leaving, even for short breaks.
4. Keep all client identified materials in locked files.
5. Move your fax machine to an area that clients and the public do not use.
6. Make sure your fax cover sheet includes a statement that notifies the receiver if confidential information is being transmitted.
7. Limit discussions of private information in informal settings, such as the receptionist area.
8. Ideally the receptionist should have an area where phone conversations cannot be overheard by clients in the waiting area.
9. Use a password-protected screensaver on your computer.
10. If you use a web deployed system that contains any protected health information, make sure your web browser is shut down before leaving your computer.
11. Lock your doors and windows before leaving your office.
12. Remember a custodian may have access to your office after hours. It is YOUR responsibility, not the custodian's, to protect your clients' information.

[TABLE OF CONTENTS] [SUMMARY]

PUBLIC LAW 104-191

AUG. 21, 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104-191
104th Congress

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**--This Act may be cited as the "Health Insurance Portability and Accountability Act of 1996".

(b) **TABLE OF CONTENTS.**--The table of contents of this Act is as follows:

...

Subtitle F--Administrative Simplification

SEC. 261. PURPOSE.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.

SEC. 262. ADMINISTRATIVE SIMPLIFICATION.

(a) IN GENERAL.--Title XI (42 U.S.C. 1301 et seq.) is amended by adding at the end the following:

"PART C--ADMINISTRATIVE SIMPLIFICATION

"DEFINITIONS

"**SEC. 1171**. For purposes of this part:

"(1) CODE SET.--The term 'code set' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

"(2) HEALTH CARE CLEARINGHOUSE.--The term 'health care clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

"(3) HEALTH CARE PROVIDER.--The term 'health care provider' includes a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)), and any other person furnishing health care services or supplies.

"(4) HEALTH INFORMATION.--The term 'health information' means any information, whether oral or recorded in any form or medium, that--

"(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

"(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

"(5) HEALTH PLAN.--The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act). Such term includes the following, and any combination thereof:

"(A) A group health plan (as defined in section 2791(a) of the Public Health Service Act), but only if the plan--

"(i) has 50 or more participants (as defined in section 3(7) of the Employee Retirement Income Security Act of 1974); or

"(ii) is administered by an entity other than the employer who established and maintains the plan.

"(B) A health insurance issuer (as defined in section 2791(b) of the Public Health Service Act).

"(C) A health maintenance organization (as defined in section 2791(b) of the Public Health Service Act).

"(D) Part A or part B of the Medicare program under title XVIII.

"(E) The medicaid program under title XIX.

"(F) A Medicare supplemental policy (as defined in section 1882(g)(1)).

"(G) A long-term care policy, including a nursing home fixed indemnity policy (unless the Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).

"(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.

"(I) The health care program for active military personnel under title 10, United States Code.

"(J) The veterans health care program under chapter 17 of title 38, United States Code.

"(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of title 10, United States Code.

"(L) The Indian health service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.).

"(M) The Federal Employees Health Benefit Plan under chapter 89 of title 5, United States Code.

"(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.--The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that--

"(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

"(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--

"(i) identifies the individual; or

"(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

"(7) STANDARD.--The term 'standard', when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174.

"(8) STANDARD SETTING ORGANIZATION.--The term 'standard setting organization' means a standard setting organization accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation of this part.

"GENERAL REQUIREMENTS FOR ADOPTION OF STANDARDS

"**SEC. 1172.** (a) APPLICABILITY.--Any standard adopted under this part shall apply, in whole or in part, to the following persons:

"(1) A health plan.

"(2) A health care clearinghouse.

"(3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).

"(b) REDUCTION OF COSTS.--Any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.

"(c) ROLE OF STANDARD SETTING ORGANIZATIONS.--

"(1) IN GENERAL.--Except as provided in paragraph (2), any standard adopted under this part shall be a standard that has been developed, adopted, or modified by a standard setting organization.

"(2) SPECIAL RULES.--

"(A) DIFFERENT STANDARDS.--The Secretary may adopt a standard that is different from any standard developed, adopted, or modified by a standard setting organization, if--

"(i) the different standard will substantially reduce administrative costs to health care providers and health plans compared to the alternatives; and

"(ii) the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5, United States Code.

"(B) NO STANDARD BY STANDARD SETTING ORGANIZATION.--If no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt under this part--

"(i) paragraph (1) shall not apply; and

"(ii) subsection (f) shall apply.

(3) CONSULTATION REQUIREMENT.--

"(A) IN GENERAL.--A standard may not be adopted under this part unless--

"(i) in the case of a standard that has been developed, adopted, or modified by a standard setting organization, the organization consulted with each of the organizations described in subparagraph (B) in the course of such development, adoption, or modification; and

"(ii) in the case of any other standard, the Secretary, in complying with the requirements of subsection (f), consulted with each of the organizations described in subparagraph (B) before adopting the standard.

"(B) ORGANIZATIONS DESCRIBED.--The organizations referred to in subparagraph (A) are the following:

"(i) The National Uniform Billing Committee.

"(ii) The National Uniform Claim Committee.

"(iii) The Workgroup for Electronic Data Interchange.

"(iv) The American Dental Association.

"(d) IMPLEMENTATION SPECIFICATIONS.--The Secretary shall establish

specifications for implementing each of the standards adopted under this

part.

"(e) PROTECTION OF TRADE SECRETS.--Except as otherwise required by law, a standard adopted under this part shall not require disclosure of trade secrets or confidential commercial information by a person required to comply with this part.

"(f) ASSISTANCE TO THE SECRETARY.--In complying with the requirements of this part, the Secretary shall rely on the recommendations of the National Committee on Vital and Health

Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)), and shall consult with appropriate Federal and State agencies and private organizations. The Secretary shall publish in the Federal Register any recommendation of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.

(g) APPLICATION TO MODIFICATIONS OF STANDARDS.--This section shall apply to a modification to a standard (including an addition to a standard) adopted under section 1174(b) in the same manner as it applies to an initial standard adopted under section 1174(a).

"STANDARDS FOR INFORMATION TRANSACTIONS AND DATA ELEMENTS

"**SEC. 1173.** (a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.--

"(1) IN GENERAL.--The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for--

"(A) the financial and administrative transactions described in paragraph (2); and

"(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

"(2) TRANSACTIONS.--The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

"(A) Health claims or equivalent encounter information.

"(B) Health claims attachments.

"(C) Enrollment and disenrollment in a health plan.

"(D) Eligibility for a health plan.

"(E) Health care payment and remittance advice.

"(F) Health plan premium payments.

"(G) First report of injury.

"(H) Health claim status.

"(I) Referral certification and authorization.

"(3) ACCOMMODATION OF SPECIFIC PROVIDERS.--The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

(b) UNIQUE HEALTH IDENTIFIERS.--

"(1) IN GENERAL.--The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the

health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

"(2) USE OF IDENTIFIERS.--The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

(c) CODE SETS.--

"(1) IN GENERAL.--The Secretary shall adopt standards that--

"(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) from among the code sets that have been developed by private and public entities; or

"(B) establish code sets for such data elements if no code sets for the data elements have been developed.

"(2) DISTRIBUTION.--The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

(d) SECURITY STANDARDS FOR HEALTH INFORMATION.--

"(1) SECURITY STANDARDS.--The Secretary shall adopt security standards that--

"(A) take into account--

"(i) the technical capabilities of record systems used to maintain health information;

"(ii) the costs of security measures;

"(iii) the need for training persons who have access to health information;

"(iv) the value of audit trails in computerized record systems; and

"(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

"(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

"(2) SAFEGUARDS.--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--

"(A) to ensure the integrity and confidentiality of the information;

"(B) to protect against any reasonably anticipated--

"(i) threats or hazards to the security or integrity of the information; and

"(ii) unauthorized uses or disclosures of the information; and

"(C) otherwise to ensure compliance with this part by the officers and employees of such person.

(e) ELECTRONIC SIGNATURE.--

"(1) STANDARDS.--The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).

"(2) EFFECT OF COMPLIANCE.--Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

(f) TRANSFER OF INFORMATION AMONG HEALTH PLANS.--The Secretary shall adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan.

"TIMETABLES FOR ADOPTION OF STANDARDS

"**SEC. 1174.** (a) INITIAL STANDARDS.--The Secretary shall carry out section 1173 not later than 18 months after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, except that standards relating to claims attachments shall be adopted not later than 30 months after such date.

"(b) ADDITIONS AND MODIFICATIONS TO STANDARDS.--

"(1) IN GENERAL.--Except as provided in paragraph (2), the Secretary shall review the standards adopted under section 1173, and shall adopt modifications to the standards (including additions to the standards), as determined appropriate, but not more frequently than once every 12 months. Any addition or modification to a standard shall be completed in a manner which minimizes the disruption and cost of compliance.

"(2) SPECIAL RULES.--

"(A) FIRST 12-MONTH PERIOD.--Except with respect to additions and modifications to code sets under subparagraph (B), the Secretary may not adopt any modification to a standard adopted under this part during the 12-month period beginning on the date the standard is initially adopted, unless the Secretary determines that the modification is necessary in order to permit compliance with the standard.

"(B) ADDITIONS AND MODIFICATIONS TO CODE SETS.--

"(i) IN GENERAL.--The Secretary shall ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets.

"(ii) Additional rules.--If a code set is modified under this subsection, the modified code set shall include instructions on how data elements of health information that were encoded prior to the modification may be converted or translated so as to preserve the informational value of the data

elements that existed before the modification. Any modification to a code set under this subsection shall be implemented in a manner that minimizes the disruption and cost of complying with such modification.

"REQUIREMENTS

"**SEC. 1175.** (a) CONDUCT OF TRANSACTIONS BY PLANS.--

"(1) IN GENERAL.--If a person desires to conduct a transaction referred to in section 1173(a)(1) with a health plan as a standard transaction--

"(A) the health plan may not refuse to conduct such transaction as a standard transaction;

"(B) the insurance plan may not delay such transaction, or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the ground that the transaction is a standard transaction; and

"(C) the information transmitted and received in connection with the transaction shall be in the form of standard data elements of health information.

"(2) SATISFACTION OF REQUIREMENTS.--A health plan may satisfy the requirements under paragraph (1) by--

"(A) directly transmitting and receiving standard data elements of health information; or

"(B) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse, and receiving standard data elements through the health care clearinghouse.

"(3) TIMETABLE FOR COMPLIANCE.--Paragraph (1) shall not be construed to require a health plan to comply with any standard, implementation specification, or modification to a standard or specification adopted or established by the Secretary under sections 1172 through 1174 at any time prior to the date on which the plan is required to comply with the standard or specification under subsection (b).

"(b) COMPLIANCE WITH STANDARDS.--

"(1) INITIAL COMPLIANCE.--

"(A) IN GENERAL.--Not later than 24 months after the date on which an initial standard or implementation specification is adopted or established under sections 1172 and 1173, each person to whom the standard or implementation specification applies shall comply with the standard or specification.

"(B) SPECIAL RULE FOR SMALL HEALTH PLANS.--In the case of a small health plan, paragraph (1) shall be applied by substituting '36 months' for '24 months'. For purposes of this subsection, the Secretary shall determine the plans that qualify as small health plans.

"(2) COMPLIANCE WITH MODIFIED STANDARDS.--If the Secretary adopts a modification to a standard or implementation specification under this part, each person to whom the standard or implementation specification applies shall comply with the modified standard or

implementation specification at such time as the Secretary determines appropriate, taking into account the time needed to comply due to the nature and extent of the modification. The time determined appropriate under the preceding sentence may not be earlier than the last day of the 180-day period beginning on the date such modification is adopted. The Secretary may extend the time for compliance for small health plans, if the Secretary determines that such extension is appropriate.

"(3) CONSTRUCTION.--Nothing in this subsection shall be construed to prohibit any person from complying with a standard or specification by--

"(A) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse; or

"(B) receiving standard data elements through a health care clearinghouse.

"GENERAL PENALTY FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS

"**SEC. 1176.** (a) GENERAL PENALTY.--

"(1) IN GENERAL.--Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.

"(2) PROCEDURES.--The provisions of section 1128A (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1128A.

"(b) LIMITATIONS.--

"(1) OFFENSES OTHERWISE PUNISHABLE.--A penalty may not be imposed under subsection (a) with respect to an act if the act constitutes an offense punishable under section 1177.

"(2) NONCOMPLIANCE NOT DISCOVERED.--A penalty may not be imposed under subsection (a) with respect to a provision of this part if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.

"(3) FAILURES DUE TO REASONABLE CAUSE.--

"(A) IN GENERAL.--Except as provided in subparagraph (B), a penalty may not be imposed under subsection (a) if--

"(i) the failure to comply was due to reasonable cause and not to willful neglect; and

"(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

"(B) EXTENSION OF PERIOD.--

"(i) NO PENALTY.--The period referred to in subparagraph (A)(ii) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure to comply.

"(ii) ASSISTANCE.--If the Secretary determines that a person failed to comply because the person was unable to comply, the Secretary may provide technical assistance to the person during the period described in subparagraph (A)(ii). Such assistance shall be provided in any manner determined appropriate by the Secretary.

"(4) REDUCTION.--In the case of a failure to comply which is due to reasonable cause and not to willful neglect, any penalty under subsection (a) that is not entirely waived under paragraph (3) may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

"WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

"**SEC. 1177.** (a) OFFENSE.--A person who knowingly and in violation of this part--

"(1) uses or causes to be used a unique health identifier;

"(2) obtains individually identifiable health information relating to an individual; or

"(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b).

"(b) PENALTIES.--A person described in subsection (a) shall--

"(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

"(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

"(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

"EFFECT ON STATE LAW

"**SEC. 1178.** (a) GENERAL EFFECT.--

"(1) GENERAL RULE.--Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall supersede any contrary provision of State law, including a provision of

State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

"(2) EXCEPTIONS.--A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall not supersede a contrary provision of State law, if the provision of State law--

"(A) is a provision the Secretary determines--

"(i) is necessary--

"(I) to prevent fraud and abuse;

"(II) to ensure appropriate State regulation of insurance and health plans;

"(III) for State reporting on health care delivery or costs; or

"(IV) for other purposes; or

"(ii) addresses controlled substances; or

"(B) subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.

"(b) PUBLIC HEALTH.--Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

"(c) STATE REGULATORY REPORTING.--Nothing in this part shall limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

"PROCESSING PAYMENT TRANSACTIONS BY FINANCIAL INSTITUTIONS

"**SEC. 1179.** To the extent that an entity is engaged in activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing,

transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

"(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.

"(2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph (1)--

"(A) for transferring receivables;

"(B) for auditing;

"(C) in connection with--

"(i) a customer dispute; or

"(ii) an inquiry from, or to, a customer;

"(D) in a communication to a customer of the entity regarding the customer's transactions, payment card, account, check, or electronic funds transfer;

"(E) for reporting to consumer reporting agencies; or

"(F) for complying with--

"(i) a civil or criminal subpoena; or

"(ii) a Federal or State law regulating the entity.".

(b) CONFORMING AMENDMENTS.--

(1) REQUIREMENT FOR MEDICARE PROVIDERS.--Section 1866(a)(1) (42 U.S.C. 1395cc(a)(1)) is amended--

(A) by striking ``and'' at the end of subparagraph (P);

(B) by striking the period at the end of subparagraph (Q) and inserting "; and"; and

(C) by inserting immediately after subparagraph (Q) the following new subparagraph:

"(R) to contract only with a health care clearinghouse (as defined in section 1171) that meets each standard and implementation specification adopted or established under part C of title XI on or after the date on which the health care clearinghouse is required to comply with the standard or specification.".

(2) TITLE HEADING.--Title XI (42 U.S.C. 1301 et seq.) is amended by striking the title heading and inserting the following:

"TITLE XI--GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION".

SEC. 263. CHANGES IN MEMBERSHIP AND DUTIES OF NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS.

Section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k))

is amended--

(1) in paragraph (1), by striking "16" and inserting "18";

(2) by amending paragraph (2) to read as follows:

"(2) The members of the Committee shall be appointed from among persons who have distinguished themselves in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. Members of the Committee shall be appointed for terms of 4 years.";

(3) by redesignating paragraphs (3) through (5) as paragraphs (4) through (6), respectively, and inserting after paragraph (2) the following:

"(3) Of the members of the Committee--

"(A) 1 shall be appointed, not later than 60 days after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, by the Speaker of the House of Representatives after consultation with the Minority Leader of the House of Representatives;

"(B) 1 shall be appointed, not later than 60 days after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, by the President pro tempore of the Senate after consultation with the Minority Leader of the Senate; and

"(C) 16 shall be appointed by the Secretary.";

(4) by amending paragraph (5) (as so redesignated) to read as follows:

"(5) The Committee--

"(A) shall assist and advise the Secretary--

"(i) to delineate statistical problems bearing on health and health services which are of national or international interest;

"(ii) to stimulate studies of such problems by other organizations and agencies whenever possible or to make investigations of such problems through subcommittees;

"(iii) to determine, approve, and revise the terms, definitions, classifications, and guidelines for assessing health status and health services, their distribution and costs, for use (I) within the Department of Health and Human Services, (II) by all programs administered or funded by the Secretary, including the Federal-State-local cooperative health statistics system referred to in subsection (e), and (III) to the extent possible as determined by the head of the agency involved, by the Department of Veterans Affairs, the Department of Defense, and other Federal agencies concerned with health and health services;

"(iv) with respect to the design of and approval of health statistical and health information systems concerned with the collection, processing, and tabulation of health statistics within the Department of Health and Human Services, with respect to the Cooperative Health Statistics System established under subsection (e), and with respect to the standardized means for the collection of health information and statistics to be established by the Secretary under subsection (j)(1);

"(v) to review and comment on findings and proposals developed by other organizations and agencies and to make recommendations for their adoption or implementation by local, State, national, or international agencies;

"(vi) to cooperate with national committees of other countries and with the World Health Organization and other national agencies in the studies of problems of mutual interest;

"(vii) to issue an annual report on the state of the Nation's health, its health services, their costs and distributions, and to make proposals for improvement of the Nation's health statistics and health information systems; and

"(viii) in complying with the requirements imposed on the Secretary under part C of title XI of the Social Security Act;

"(B) shall study the issues related to the adoption of uniform data standards for patient medical record information and the electronic exchange of such information;

"(C) shall report to the Secretary not later than 4 years after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996 recommendations and legislative proposals for such standards and electronic exchange; and

"(D) shall be responsible generally for advising the Secretary and the Congress on the status of the implementation of part C of title XI of the Social Security Act."; and

(5) by adding at the end the following:

"(7) Not later than 1 year after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, and annually thereafter, the Committee shall submit to the Congress, and make public, a report regarding the implementation of part C of title XI of the Social Security Act. Such report shall address the following subjects, to the extent that the Committee determines appropriate:

"(A) The extent to which persons required to comply with part C of title XI of the Social Security Act are cooperating in implementing the standards adopted under such part.

"(B) The extent to which such entities are meeting the security standards adopted under such part and the types of penalties assessed for noncompliance with such standards.

"(C) Whether the Federal and State Governments are receiving information of sufficient quality to meet their responsibilities under such part.

"(D) Any problems that exist with respect to implementation of such part.

"(E) The extent to which timetables under such part are being met.".

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(a) IN GENERAL.--Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on

Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) SUBJECTS FOR RECOMMENDATIONS.--The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

(c) REGULATIONS.--

(1) IN GENERAL.--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).

(2) PREEMPTION.--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.

(d) CONSULTATION.--In carrying out this section, the Secretary of Health and Human Services shall consult with--

(1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and

(2) the Attorney General.

...

HCPCS Temporary National Coding decisions for 2003

(These items will appear in the 2004 HCPCS Update)

I. THE FOLLOWING LISTING OF HCPCS NATIONAL CODES WERE ESTABLISHED IN 2002, BUT INADVERTANLY LEFT OUT OF THE 2003 HCPCS UPDATE AS POSTED ON THE WEB ON OCTOBER 21, 2002. WE APOLOGIZE FOR ANY INCONVENIENCE. PLEASE INCLUDE THE FOLLOWING IN THE LIST OF NATIONAL HCPCS CODES AND MODIFIERS FOR USE IN 2003

"S" modifiers ADDED effective 7/1/2002

SM – Second surgical opinion
(Short Description: Second opinion)

SN – Third surgical opinion
(Short Description: Third Opinion)

"S" CODES ADDED effective July 1, 2002:

S9484 Crisis intervention mental health services, per hour
(Short Description: Crisis intervention per hour)

S9490 Home infusion therapy, corticosteroid infusion; administrative services, professional pharmacy services, care coordination, and all necessary supplies and equipment (drugs and nursing visits coded separately), per diem
(Short Description: HIT corticosteroid diem)

S9806 RN services in the infusion suite of the IV therapy provider, per visit
(Short Description: RN infusion suite visit)

S9900 Services by authorized Christian Science Practitioner for the process of healing, per diem. Not to be used for rest or study. Excludes in-patient services.
(Short Description: Christian Sci Pract visit)

"S" MODIFIER ADDED effective 10/1/2002

SQ Item ordered by home health

"S" CODES ADDED effective October 1, 2002

S0104 Zidovudine, oral, 100 mg

S0135 Injection, pegfilgrastim, 6 mg

S0201 Partial hospitalization services, less than 24 hours, per diem

S0207 Paramedic intercept, non-hospital-based ALS service (non-voluntary), non-transport

S0315 Disease management program; initial assessment and initiation of the program

S0316 follow-up/reassessment

S0320 Telephone calls by a registered nurse to a disease management program member for monitoring purposes; per month

S1040 Cranial remolding orthosis, rigid, with soft interface material, custom fabricated, includes fitting and adjustment(s)

S2262 Abortion for maternal indication, 25 weeks or greater

S2265 Abortion for fetal indication, 25-28 weeks

S2266 Abortion for fetal indication, 29-31 weeks

S2267 Abortion for fetal indication, 32 weeks or greater

S3655 Antisperm antibodies test (immunobead)

S8004 Radioimmunopharmaceutical localization of targeted cells; whole body

S codes ADDED effective 1/1/2003

S5100 Day care services, adult; per 15 minutes

S5101 per half day

S5102 per diem

S5105 Day care services, center-based; services not included in program fee, per diem

S5110 Home care training, family; per 15 minutes

S5111 per session

S5115 Home care training, non-family; per 15 minutes

S5116 per session

S5120 Chore services; per 15 minutes

S5121 per diem

S5125 Attendant care services; per 15 minutes

S5126 per diem

S5130 Homemaker service, NOS; per 15 minutes

S5131 per diem

S5135 Companion care, adult (e.g. IADL/ADL); per 15 minutes

S5136 per diem

S5140 Foster care, adult; per diem

S5141 per month

S5145 Foster care, therapeutic, child; per diem

S5146 per month

S5150 Unskilled respite care, not hospice; per 15 minutes

S5151 per diem

S5160 Emergency response system; installation and testing

S5161 service fee, per month (excludes installation and testing)

S5162 purchase only

S5165 Home modifications; per service

S5170 Home delivered meals, including preparation; per meal

S5175 Laundry service, external, professional; per order

S5180 Home health respiratory therapy, initial evaluation

S5181 Home health respiratory therapy, NOS, per diem

S5185 Medication reminder service, non-face-to-face; per month

S5190 Wellness assessment, performed by non-physician

S5199 Personal care item, NOS, each

Please correct TYPO - Code S9150 was incorrectly entered as S9105.
The code is S9150 EVALUATION BY OCCULARIST added effective 4/1/2002

"S" CODE DELETED EFFECTIVE 12/31/02. PLEASE MAKE THE CORRECTION TO YOU DATABASE.

S8433 discontinued 12/31/2002 and cross-walked to code A4280

(The following "T" code appeared on the 2002 list of Temporary Codes. The code is however being deleted – removed from the HCPCS as if it never existed because the National Panel made the decision to establish a National "A" code in its place. The code does not appear in the 2003 HCPCS.)

DELETED 12/31/02: T1501 UNDERPAD, REUSABLE/WASHABLE, ANY SIZE, EACH (Short description: Reusable underpad)

II. THE FOLLOWING NEWLY ESTABLISHED CMS MODIFIERS AND CODES ARE BEING ADDED EFFECTIVE JANUARY 1, 2003. THEY DID NOT APPEAR IN THE 2003 HCPCS UPDATE AS POSTED ON THE WEB ON OCTOBER 10, 2002. PLEASE ADD TO YOUR 2003 HCPCS DATABASE

"Q" Code added effective January 1, 2003

Q3000 SUPPLY OF RADIOPHARMACEUTICAL DIAGNOSTIC IMAGING AGENT, RUBIDIUM RB-82, PER DOSE
(Short description: Rubidium RB-82)

CMS Modifiers added effective January 1, 2003

CA PROCEDURE PAYABLE ONLY IN THE INPATIENT SETTING WHEN PERFORMED EMERGENT ON AN OUTPATIENT WHO EXPIRES PRIOR TO ADMISSION
Short Description = Procedure payable inpatient)

CB SERVICE ORDERED BY A RENAL DIALYSIS FACILITY (RDF) PHYSICIAN AS PART OF THE BENEFICIARY'S BENEFIT, IS NOT PART OF THE COMPOSIT RATE, AND IS SEPARATELY REIMBURSABLE
(SHORT description = Separately reimbursable serv

********** **11/7/02/ckr**

III. THE FOLLOWING HCPCS CODES AND MODIFIERS ARE BEING ADDED, REVISED, OR DISCONTINUED. EFFECTIVE DATES ARE AS SPECIFIED BELOW. THESE MODIFICATIONS TO THE HCPCS SYSTEM DID NOT APPEAR IN THE 2003 HCPCS UPDATE, AS POSTED ON OCTOBER 22, 2002 AT http://www.cms.hhs.gov/medicare/providers/pufdownload/anhcpcdl.asp PLEASE MAKE THE APPROPRIATE CHANGES TO YOUR 2003 HCPCS DATABASE.

"A" Codes modified effective April 1, 2003

A4232 Change payment indicator to "i"

A4632 Change payment indicator to "i"

"C" modifier revised, effective April 1, 2003

CB Language of long and short descriptions revised to read as follows:
SERVICE ORDERED BY A RENAL DIALYSIS FACILITY (RDF) PHYSICIAN AS PART OF THE **ESRD** BENEFICIARY'S **DIALYSIS** BENEFIT, IS NOT PART OF THE COMPOSIT**E** RATE, AND IS SEPARATELY REIMBURSABLE
Short Description: ESRD bene part A SNF-sep pay

In addition, the effective date of the above code is changed from January 1, 2003 to April 1, 2003.

"C" Code added effective January 1, 2003

C1884 EMBOLIZATION PROTECTIVE SYSTEM
Short Description: Embolization protect syst

"G" Code discontinued effective March 31, 2003 (Refer to replacement code Q3031)

G0025 COLLAGEN SKIN TEST KIT
Short Description: Collagen skin test kit

"G" modifier added effective April 1, 2003

GF	NON-PHYSICIAN (E.G. NURSE PRACTITIONER (NP), CERTIFIED REGISTERED NURSE ANESTHETIST (CRNA), CERTIFIED REGISTERED NURSE (CRN), CLINICAL NURSE SPECIALIST (CNS), PHYSICIAN ASSISTANT (PA)) SERVICES IN A CRITICAL ACCESS HOSPITAL Short Description: Nonphysician serv C A Hosp

"G" Code discontinued effective March 31, 2003

G0025

"G" Code cancelled for implementation effective January 1, 2003

G0296

"H" Codes added effective April 1, 2003

H2010	Comprehensive Medication Services, per 15 minutes Short Description: Comprehensive med svc 15 min
H2011	Crisis Intervention Service, per 15 minutes Short Description: Crisis interven svc, 15 min
H2012	Behavioral Health Day Treatment, per hour Short Description: Behav Hlth Day Treat, per hr
H2013	Psychiatric health facility service, per diem Short Description: Psych hlth fac svc, per diem
H2014	Skills Training and Development, per 15 minutes Short Description: Skills Train and Dev, 15 min
H2015	Comprehensive Community Support Services, per 15 minutes Short Description: Comp Comm Supp Svc, 15 min
H2016	Comprehensive Community Support Services, per diem Short Description: Comp Comm Supp Svc, per diem
H2017	Psychosocial Rehabilitation Services, per 15 minutes Short Description: PsySoc Rehab Svc, per 15 min

H2018	Psychosocial Rehabilitation Services, per diem Short Description: PsySoc Rehab Svc, per diem
H2019	Therapeutic Behavioral Services, per 15 minutes Short Description: Ther Behav Svc, per 15 min
H2020	Therapeutic Behavioral Services, per diem Short Description: Ther Behav Svc, per diem
H2021	Community-Based Wrap-Around Services, per 15 minutes Short Description: Com Wrap-Around Sv, 15 min
H2022	Community-Based Wrap-Around Services, per diem Short Description: Com Wrap-Around Sv, per diem
H2023	Supported Employment, per 15 minutes Short Description: Supported Employ, per 15 min
H2024	Supported Employment, per diem Short Description: Supported Employ, per diem
H2025	Ongoing Support to Maintain Employment, per 15 minutes Short Description: Supp Maint Employ, 15 min
H2026	Ongoing Support to Maintain Employment, per diem Short Description: Supp Maint Employ, per diem
H2027	Psychoeducational Service, per 15 minutes Short Description: Psychoed Svc, per 15 min
H2028	Sexual Offender Treatment Service, per 15 minutes Short Description: Sex Offend Tx Svc, 15 min
H2029	Sexual Offender Treatment Service, per diem Short Description: Sex Offend Tx Svc, per diem
H2030	Mental Health Clubhouse Services, per 15 minutes Short Description: MH Clubhouse Svc, per 15 min
H2031	Mental Health Clubhouse Services, per diem Short Description: MH Clubhouse Svc, per diem
H2032	Activity Therapy, per 15 minutes Short Description: Activity Therapy, per 15 min

H2033	Multisystemic Therapy for juveniles, per 15 minutes Short Description: Multisys Ther/Juvenile 15min
H2034	Alcohol and/or Drug Abuse Halfway House Services, per diem Short Description: A/D Halfway House, per diem
H2035	Alcohol and/or Other Drug Treatment Program, per hour Short Description: A/D Tx Program, per hour
H2036	Alcohol and/or Other Drug Treatment Program, per diem Short Description: A/D Tx Program, per diem
H2037	Developmental Delay Prevention Activities, Dependent Child of Client, per 15 minutes Short Description: Dev Delay Prev Dp Ch, 15 min

"K" Codes added effective April 1, 2003

K0552	SUPPLIES FOR EXTERNAL INFUSION PUMP, SYRINGE TYPE CARTRIDGE, STERILE, EACH
K0560	METACARPAL PHALANGEAL JOINT REPLACEMENT, TWO PIECES, METAL (E.G., STAINLESS STEEL OR COBALT CHROME), CERAMIC-LIKE MATERIAL (E.G., PYROCARBON), FOR SURGICAL IMPLANTATION (ALL SIZES, INCLUDES ENTIRE SYSTEM)
K0600	FUNCTIONAL NEUROMUSCULAR STIMULATOR, TRANSCUTANEOUS STIMULATOIN OF MUSCLES OF AMBULATION WITH COMPUTER CONTROL, USED FOR WALKING BY SPINAL CORD INJURED, ENTIRE SYSTEM, AFTER COMPLETION OF TRAINING PROGRAM Short Description: Functional neruomuscularstim
K0601	REPLACEMENT BATTERYFOR EXTERNAL INFUSION PUMP OWNED BY PATIENT, SILVER OXIDE, 1.5 VOLT, EACH Short Description: Repl batt silver oxide 1.5 v
K0602	REPLACEMENT BATTERY FOR EXTERNAL INFUSION PUMP OWNED BY PATIENT, SILVER OXIDE, 3 VOLT, EACH Short Description: Repl batt silver oxide 3 v
K0603	REPLACEMENT BATTERY FOR EXTERNAL INFUSION PUMP OWNED BY PATIENT, ALKALINE, 1.5 VOLT, EACH Short Description: Repl batt alkaline 1.5 v

K0604 REPLACEMENT BATTERY FOR EXTERNAL INFUSION PUMP OWNED BY PATIENT, LITHIUM, 3.6 VOLT, EACH
Short Description: Repl batt lithium 3.6 v

K0605 REPLACEMENT BATTERY FOR EXTERNAL INFUSION PUMP OWNED BY PATIENT, LITHIUM, 4.5 VOLT, EACH
Short Description: Repl batt lithium 4.5 v

"K" Codes modified effective April 1, 2003

K0455 Language revised to read:
INFUSION PUMP USED FOR UNINTERRUPTED PARENTERAL ADMINISTRATION OF MEDICATION, EPOPROSTENOL OR TREPROSTINOL

"Q" Code added effective April 1, 2003, to replace G Code G0025, (discontinued effective March 31, 2003). The alpha-numeric designation is changed in order to place the code at the appropriate place in the system, because the test is a supply, not a service.

Q3031 COLLAGEN SKIN TEST
Short Description: Collagen skin test

"Q" Codes discontinued effective January 1, 2003

Q3021
Q3022
Q3023

"S" code changes effective 4/1/2003

Delete the following S codes:

S8945

S9524

Add the following S codes:

S0136 Clozapine, 25 mg
Short Description: Clozapine, 25 mg

S0137 Didanosine (ddI), 25 mg

Short Description: Didanosine, 25 mg

S0138 Finasteride, 5 mg
Short Description: Finasteride, 5 mg

S0139 Minoxidil, 10 mg
Short Description: Minoxidil, 10 mg

S0140 Saquinavir, 200 mg
Short Description: Saquinavir, 200 mg

S0141 Zalcitabine (ddC), 0.375 mg
Short Description: Zalcitabine, 0.375 mg

S2090 Ablation, open, one or more renal tumor(s); cryosurgical
Short Description: Open cryosurg renal

S2091 Ablation, percutaneous, one or more renal tumor(s); cryosurgical
Short Description: Perc cryosurg renal

S3000 Diabetic indicator; retinal eye exam, dilated, bilateral
Short Description: Bilat dil retinal exam

S3820 Complete BRCA1 and BRCA2 gene sequence analysis for susceptibility to breast and ovarian cancer
Short Description: Comp BRCA1/BRCA2

S3822 Single-mutation analysis (in individual with a known BRCA1 or BRCA2 mutation in the family) for susceptibility to breast and ovarian cancer
Short Description: Sing mutation brst/ovar

S3823 Three-mutation BRCA1 and BRCA2 analysis for susceptibility to breast and ovarian cancer in Ashkenazi individuals
Short Description: 3 mutation brst/ovar

S3828 Complete gene sequence analysis; MLH1 gene
Short Description: Comp MLH1 gene

S3829 MSH2 gene
Short Description: Comp MSH2 gene

S3833 Complete APC gene sequence analysis for susceptibility to familial adenomatous polyposis (FAP) and attenuated FAP
Short Description: Comp APC sequence

S3834 Single-mutation analysis (in individual with a known APC mutation in

the family) for susceptibility to familial adenomatous polyposis (FAP) and attenuated FAP
Short Description: Sing mutation APC

S5108 Home care training to home care client, per 15 minutes
Short Description: Homecare train pt 15 min

S5109 per session
Short Description: Homecare train pt session

S8460 Camisole, post-mastectomy
Short Description: Camisole post-mast

S8990 Physical or manipulative therapy performed for maintenance rather than restoration
Short Description: PT or manip for maint

S9434 Modified solid food supplements for inborn errors of metabolism
Short Description: Mod solid food suppl

"T" Codes added effective April 1, 2003

T2010 Preadmission Screening and Resident Review (PASRR) Level I Identification Screening, per screen
Short Description: PASRR LEVEL I

T2011 Preadmission Screening and Resident Review (PASRR) Level II Evaluation, per evaluation
Short Description: PASRR LEVEL II

"T" Codes discontinued effective March 31, 2003

T1011 Discontinue existing HCPCS code T1011, because it is duplicative of code H0047, (which was newly established for 2003).

T1008 Discontinue existing HCPCS code T1008, because it is duplicative of newly established code H2012 that will be effective April 1, 2003.

"U" Modifiers added effective April 1, 2003

UF MORNING
Short Description: Morning

UG	AFTERNOON Short Description: Afternoon
UH	EVENING Short Description: Evening
UJ	NIGHT Short Description: Night
UK	SERVICES PROVIDED ON BEHALF OF THE CLIENT TO SOMEONE OTHER THAN THE CLIENT (COLLATERAL RELATIONSHIP) Short Description: Svc on behalf client-collat.

********** **12/20/02/csh**

HIPAA WEB RESOURCES

There are literally hundreds of web sites that offer assistance with HIPAA compliance. Use your favorite search engine with the keyword "hipaa." Some web sites offer their services only for a fee, so be cautious. While you can spend a lot of time surfing the web looking for HIPAA materials, most if not all the tools you need for the Privacy Rule and the Codes and Transactions Rule are already available to you through this manual and its attachments.

Listed below are several of the web sites used to develop this manual.

www.hhs.gov/ocr/hipaa
www.samhsa.gov/hipaa
www.mhccm.org
www.cms.gov/hipaa
www.cms.hhs.gov/hipaa
www.hipaadvisory.com
www.hipaainfo.net/status.htm
www.hipaa-iq.com/summary.htm
www.emabenefits.com/HIPAA.htm
www.KnowledgeStorm.com
www.wpc-edi.com/hipaa
www.aspe.hhs.gov/admnsimp
www.fyi-hipaa.com
www.hipaanet.com
www.medscout.com/hipaa
www.firstgov.gov

Most state governments also have a web site for HIPAA. Go to www.colorado.gov, click on "Government" in the column on the left, scroll down and click on "Other State Governments."

REQUEST FOR PROTECTED HEALTH INFORMATION (PHI)

Patient name: _____ Date of birth:_____

Patient number:_____

Patient address:_____

_____

Information requested:

_____
_____
_____
_____
_____

Date requested: _____

Signature: _____

For Healthcare Organization Use Only:

Date received_____ Request has been Accepted Denied

If denied, check reason for denial:

- ❑ PHI was not created by this organization.
- ❑ PHI is not a part of patient's designated record set.
- ❑ PHI is not available to the patient for inspection as required by federal law.
- ❑ PHI may be obtained from: _____
  _____
  _____

Signature _____