HIPAA MANUAL
Updated August 2004

This manual was compiled by the Alcohol and Drug Abuse Division HIPAA Workgroup during the summer and fall of 2002 and updated in August 2004.. 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. The National Provider Identifier and the Security Rule have also been publilshed. 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.

There are two HIPAA resources that ADAD has found to be vital. Both are specifically for alcohol and substance abuse providers.
1) The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs, June 2004. This is available at www.samhsa.gov
2) Confidentiality and Communication: A Guide to the Federal Drug & Alcohol Confidentiality Law and HIPAA, 2003 Edition. Legal Action Committee 1-800-783-4903

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 Alcohol and Drug Abuse Division at 4055 S. Lowell Blvd., Denver, CO 80236, 303-866-7480. There is a cost for copying. All attachments are included with the paper copy. It is also available free of charge on the ADAD web site at www.cdhs.state.co.us/ohr/adad/index.html. 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	10/16/03
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	April 20, 2005
National Provider Identifier	published 5/7/98	published 1/23/04	5/23/07
National Employer Identifier	published 6/16/01	not yet published	
National Health Plan Identifier	not yet published	not yet published	
National Individual Identifier	not yet published	on hold	on hold
Claims Attachment	not yet published	not yet published	
Enforcement	not yet published	not yet published	

HIPAA and Other Laws
In summary, HIPAA does 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. **For all alcohol and substance abuse providers** - HIPAA and 42 CFR Part 2 (Confidentiality of Alcohol and Drug Abuse records)

   You must comply with whichever part of HIPAA and 42 CFR is more stringent.

   The Legal Action Center has published a crosswalk between HIPAA and 42 CFR, identifying which specific parts of each are the more stringent. You may order a copy of this document from the Legal Action Center at 1-800-223-4044. There is a purchase cost.

The Substance Abuse and Mental Health Administration (SAMHSA) at the U.S. Department of Health and Human Services has developed a HIPAA-42 CFR Part 2 crosswalk, which is available for download from their web site at: http://www.samhsa.gov.

3. **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.

For alcohol and substance abuse providers, 42 C.F.R. Part 2 does not contain a parallel provision. The Legal Action Center in the Guide to the Federal Drug & Alcohol Confidentiality Law, recommends all providers:
a) develop appropriate "duty to warn" policies with the assistance of an attorney knowledgeable with state law,
b) ensure their policies comply with federal confidentiality regulations which take precedence over conflicting state law, and
c) ensure your insurance policies cover claims that might arise from "duty to warn" situations.

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
- computerized faxes

"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.

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 not 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.

What you need to do:

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 CoveredTransactions

- 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.