THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996: A SUMMARY OF REGULATORY REQUIREMENTS

TABLE OF CONTENTS

HIPAA: THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

I. What is HIPAA?

HIPAA is a federal law passed by Congress in 1996 for the purpose of improving the portability and continuity of health insurance coverage, to combat waste, fraud and abuse in health insurance and health care delivery, to simplify the administration of health insurance, and for other purposes.

In order to achieve the goal of administrative simplification and to encourage the development of a health information system, HIPAA calls for the establishment of standards and requirements for the electronic transmission of certain health information.

II. Administrative Simplification

HIPAA requires the U.S. Department of Health and Human Services (DHHS) to establish standards in the following areas:

A. Transactions
B. Unique Health Identifiers
C. Security
D. Privacy of Health Information

III. Who Must Comply with HIPAA?

The Standards adopted by DHHS apply to the following "covered entities:"

F. A health plan
G. A health care clearinghouse
H. A health care provider who transmits any health information in electronic form in connection with a covered transaction.

Health Plan means an individual or group plan that provides, or pays the cost of, medical care. A **health plan** includes a group health plan, defined as an employee welfare benefit plan (ERISA) that has 50 or more participants or is administered by an entity other than the employer that established and maintains the plan.

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, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

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

1) preventative, 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.

IV Covered Transactions

A. In General

A **Covered Transaction** is 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 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 which DHHS may prescribe by regulation.

If a Covered Entity conducts with another Covered Entity (or within the same Covered Entity), using electronic media, a transaction for which DHHS has adopted a standard, the Covered Entity must conduct the transaction as a standard transaction.

B. Business Associates

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: 1) comply with all applicable transactions requirements and 2) require any agent or subcontractor to comply with all applicable transactions requirements.

Business Associate means, with respect to a Covered Entity, a person who:

(i) on behalf of such Covered Entity or an Organized Health Care Arrangement ("OHCA"), but other than in the capacity of a member of the workforce of such Covered Entity, 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 HIPAA; or

(ii) Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity or an OHCA, where the provision of the service involves the disclosure of individually identifiable health information from such Covered Entity or OHCA, or from another Business Associate of such Covered Entity or OHCA, to the person.

A Covered Entity participating in an OHCA that performs a function, activity or service as described in (i) or (ii) above, does not because of that performance become a business associate of the other covered entities in the OHCA.

A Covered Entity may be a Business Associate of another Covered Entity.

When conducting a covered transaction, a Covered Entity must use the applicable medical data code sets as specified in the implementation specifications adopted by DHHS that are valid at the time the health care is furnished and the nonmedical data code sets as specified in the implementation specifications adopted by DHHS that are valid at the time the transaction is initiated.

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. It includes the codes and descriptors of the codes.

A Covered Entity may not enter into an trading partner agreement (an agreement related to the exchange of information in electronic transactions between each party to the agreement) that would change the definition, data condition or data element or segment in a standard; add any data elements or segments to the maximum defined data set; 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); or change the meaning or intent of the standard's implementation specification(s).

C. <u>Additional Requirements for Health Plans</u>

6. If an entity requests a health plan to conduct a transaction as a standard transaction, the health plan must do so.
7. A health plan may not reject a transaction, or attempt to adversely affect the other entity or transaction because it is a standard transaction.
8. 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.
9. A health plan may not offer an incentive to a health care provider to conduct a transaction as a direct data entry transaction.
10. 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.
11. If a health plan receives a standard transaction and coordinates benefits with another health plan or payer, it must store the coordination of benefits data it needs to forward the standard transaction to the other health plan or payer.
12. A health plan must accept and promptly process any standard transaction that contains codes that are valid.
13. A health plan must keep code sets for the current billing period and appeals periods still open to processing under the terms of the health plan's coverage.

D. Compliance Date

The Compliance Date for the Transaction Standards is October 16, 2002. However, recently passed legislation allows covered entities to apply for an extension of this deadline to delay compliance until October 16, 2003. The University applied for this extension.

V. Privacy of Health Information

A. General Requirements

The privacy regulations under HIPAA apply to covered entities who transmit health information in electronic form in connection with a covered transaction.

1. Use and Disclosure

A Covered Entity may not use or disclose protected health information except as permitted or required under HIPAA.

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.

Individually identifiable health information means 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.

Protected health information ("PHI") means individually identifiable health information:

1) Except as provided in (2) of this definition, that is:
   (i) transmitted by electronic media;

   (ii) maintained in any medium described in the definition of electronic media; or

   (iii) transmitted or maintained in **any other form or medium**

2) PHI excludes individually identifiable health information in:

   (i) Education records covered by **FERPA**; and

   (ii) Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.

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

Electronic Media means the mode of electronic transmission, including the Internet, Extranet, 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.

a. <u>Permitted Uses and Disclosures of PHI</u>

i. To the individual;
ii. For treatment, payment or health care operations as permitted by the regulations;
iii. Pursuant to and in compliance with an Authorization
iv. Pursuant to an agreement or in an emergency
v. Other uses as permitted by the regulations
vi. Incident to a use or disclosure otherwise permitted or required by the regulations

b. Required Disclosures of PHI

i. To the individual when requested
ii. When required by the Secretary of DHHS for compliance purposes

2. Minimum Necessary Rule

When using or disclosing PHI or when requesting PHI 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.

This rule does not apply to:

a. Disclosures to or requests by a health care provider for treatment;
b. Uses or disclosures made to the individual;
c. Uses or disclosures made pursuant to an authorization;
d. Disclosures made to the Secretary for compliance and enforcement;
e. Uses or disclosures required by law; and
f. Uses and disclosures that are required for compliance with HIPAA requirements

2. Business Associates

A Covered Entity may disclose PHI to a Business Associate and may allow a Business Associate to create or receive PHI on its behalf, if the Covered Entity obtains satisfactory assurance that the Business Associate will appropriately safeguard the information. Examples of a Business Associate include billing companies, computer vendors, accrediting organizations, administrative service providers, accountants, attorneys, auditors, consultants and document storage or destruction companies.

b. Exceptions

This standard does not apply:

i. With respect to disclosures by a Covered Entity to a health care provider concerning treatment;
ii. With respect to disclosures by a group health plan, a health insurance

issuer or HMO with respect to a group health plan to the plan sponsor if the requirements of 164.504(f) are met; or
iii. With respect to uses or disclosures by a health plan that is a government program providing public benefits.

b. Business Associate Contracts

The contract between the Covered Entity and the Business Associate must 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 HIPAA if done by the Covered Entity, except that the contract may permit the Business Associate to use and disclose PHI for its own management and administration, and may permit the Business Associate to provide data aggregation services relating to the health care operations of the Covered Entity.

The DHHS has provided sample business associate contract language in an appendix to the regulations to assist Covered Entities in complying with the requirements.

4. Deceased Individuals

A Covered Entity must comply with the requirements of the privacy regulations with respect to the PHI of a deceased individual.

4. Personal Representatives

Except as otherwise provided, a Covered Entity must treat a personal representative as the individual for purposes of privacy of PHI.

b. Adults and Emancipated Minors

If under applicable law, a person has the authority to act on behalf of an adult or emancipated minor in making decisions related to health care, a Covered Entity must treat the person as a personal representative with respect to PHI relevant to such personal representation.

b. Unemancipated Minors

If under applicable law, a parent, guardian or other person acting in loco parentis has the authority to act on behalf of an unemancipated minor in making decisions related to health care, a Covered Entity must treat the person as a personal representative with respect to PHI relevant to such personal representation, except that such person may not be a personal representative and the minor has the authority to act as an individual with

respect to PHI if:

i. The minor consents to such health care service, no other consent is required by law, and the minor has not requested such person be treated as the personal representative;

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 agrees to confidentiality between a covered health care provider and the minor.

Notwithstanding the above provisions, if applicable state or other law permits or requires disclosure of PHI of an unemancipated minor to a parent, guardian or other person acting in loco parentis, a Covered Entity may disclose the PHI; if applicable state or other law prohibits disclosure of PHI of an unemancipated minor to a parent, guardian or other person acting in loco parentis, a Covered Entity may not disclose the PHI; and where the parent, guardian or other person acting in loco parentis is not the personal representative under the above provisions and there is no applicable access provision under state or other law, a Covered Entity may provide or deny access to PHI to a parent, guardian or other person acting in loco parentis if such action is consistent with state or other applicable law and the decision is made by a licensed health care professional.

b. Deceased Individuals

If under applicable law, an executor, administrator, or other person has the authority to act on behalf of a deceased individual or of the individual's estate, a Covered Entity must treat the person as a personal representative with respect to PHI relevant to such personal representation.

b. Abuse, Neglect and Endangerment Situations

Notwithstanding any state law or any HIPAA requirement to the contrary, a Covered Entity may elect not to treat a person as the personal representative of an individual if:

i. The individual has been or may be subjected to domestic violence, abuse or neglect by such person; or

ii. Treating such person as the personal representative could endanger

the individual; and

iii. The Covered Entity decides, in the exercise of professional judgment, that it is not in the individual's best interest to treat the person as the personal representative.

6. Whistleblowers and Crime Victims

A Covered Entity is not considered to have violated the requirements of the Privacy regulations if a member of its workforce or a Business Associate discloses PHI because of a reasonable belief that the Covered Entity engaged in unlawful or unprofessional conduct or provided care that endangers one or more patients, workers or the public, and the disclosure is to a health oversight agency, an authorized public health authority, an appropriate health care accreditation organization, or an attorney retained by the employee or Business Associate to determine their legal options.

A Covered Entity is not considered to have violated the requirements of the Privacy regulations if a member of its workforce who is a victim of a criminal act discloses PHI to a law enforcement official if the PHI disclosed is about the suspected perpetrator of the criminal act and the PHI disclosed is limited to certain information specified in the regulations.

B. **Uses and Disclosures : Organizational Requirements**

1. Hybrid Entities

If a Covered Entity is a Hybrid Entity, the requirements of the Privacy regulations, other than these Organizational Requirements, apply only to the Health Care Component(s) of the Hybrid Entity.

Hybrid Entity means a single legal entity that is a Covered Entity whose business activities include both covered and non-covered functions and who designates health care components in accordance with the regulations. The University of Maine System is a Hybrid Entity.

Health Care Component means: A component or combination of components of a Hybrid Entity designated and documented by the Hybrid Entity. The Health Care Component must include any component that would meet the definition of Covered Entity if it were a separate legal entity. The Health Care Component may also include a component only to the extent it performs:

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

The Covered Entity that is a Hybrid Entity must ensure that the Health Care Component of the entity complies with the Privacy regulations. The Hybrid Entity must ensure that:

a. Its health care component does not disclose PHI to another component of the Covered Entity in circumstances which would be prohibited by the Privacy regulations if the health care component and the other component were distinct legal entities.

b. A component that performs activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities does not use or disclose PHI it creates or receives from or on behalf of the health care component in a way prohibited by the Privacy regulations.

c. If a member of the workforce performs duties for the health care component and another component of the entity, such person must not use or disclose PHI created or received in the course of or incident to the person's work for the health care component in a way prohibited by the Privacy regulations.

d. It complies with the Privacy regulations.

e. Policies and procedures ensuring compliance with the Privacy regulations are implemented.

f. The components that are part of the health care component are designated and that such designation is documented as required.

2. Requirements for Group Health Plans

Except as provided in the second and third paragraphs below or otherwise authorized by the individual, a group health plan may not disclose PHI to the plan sponsor or provide for or permit the disclosure of PHI to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan unless the plan documents restrict the uses and disclosures of such information by the plan sponsor consistent with the requirements of the Privacy regulations.

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 purposes of 1) obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or 2) modifying, amending, or terminating the group health plan.

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 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.

Plan documents must be amended to incorporate provisions which establish the permitted uses and disclosures of such information by the plan sponsor, must provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification from the plan sponsor that the plan documents have been amended to incorporate the provisions required by the Privacy regulations, and must provide for adequate separation between the group health plan and the plan sponsor.

A group health plan may not disclose PHI 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.

2. Multiple Covered Functions

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 Privacy regulations as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

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

C. **Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations**

Except for uses or disclosures of psychotherapy notes and uses or disclosures for marketing purposes, a Covered Entity may use or disclose PHI for treatment, payment or health care operations, provided such use or disclosure is consistent with other applicable requirements of the Privacy regulations, as follows:

1. A Covered Entity may use or disclose PHI for its own treatment, payment or health care operations.
2. A Covered Entity may disclose PHI for treatment activities of a health care provider.
3. A Covered Entity may disclose PHI 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 PHI 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 PHI being requested, the PHI pertains to such relationship, and the disclosure is for the purpose of conducting quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, evaluating provider performance and conducting training programs, or health care fraud and abuse detection or compliance.
    2. A Covered Entity that is in an OHCA may disclose PHI to another Covered Entity in the OHCA for any health care operations activities of the OHCA.

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

Payment means the activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or the activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Health Care Operations means any of the following activities of the Covered Entity to the extent the activities are related to covered functions:

1. Conducting quality assessment and improvement activities
2. Reviewing the competence or qualifications of health care professionals, evaluating provider performance and conducting training programs
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance
4. Conducting or arranging for medical review, legal services and auditing functions
5. Business planning and development
6. Business management and general administrative duties of the entity

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.

D. **Uses and Disclosures for which an Authorization is Required**

1. General Rule

Except as otherwise permitted by the Privacy regulations, a Covered Entity may not use or disclose PHI without a valid authorization.

1. Psychotherapy Notes

Notwithstanding any other provision of the Privacy Regulations, except for the transition provisions, a Covered Entity must obtain an authorization for any use or disclosure of psychotherapy notes, except for:

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 counseling;
c. Use or disclosure by the Covered Entity to defend itself in a legal action or other proceeding brought by the individual; or
d. A Use or disclosure that is required by the DHHS, required by law, required by court order with respect to the oversight of the originator of the psychotherapy notes, is permitted to a coroner or medical examiner to identify a deceased person or cause of death, or as is necessary to avert a serious and imminent threat to the health or safety of a

person or the public.

3. Marketing

Notwithstanding any other provision of the Privacy Regulations, except for the transition provisions, a Covered Entity must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

b. A face-to-face communication made by a Covered Entity to an individual; or
c. A promotional gift of nominal value provided by the Covered Entity.

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.

3. Valid Authorizations

A valid authorization must contain the following elements:

b. A specific and meaningful description of the information to be used or disclosed;
c. The name or other specific identification of the person(s) authorized to make the requested use or disclosure;
d. The name or other specific identification of the person(s) to whom the Covered Entity may make the requested use or disclosure;
e. A description of each purpose of the requested use or disclosure;
f. An expiration date or event that relates to the individual or the purpose of the use or disclosure. The statement “end of research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of PHI for research;
g. Signature of the individual and date. If signed by a personal representative, a description of such representative’s authority to act must be included;
h. Notice of the individual’s right to revoke the authorization in writing, the exceptions to the right to revoke and a description of how to revoke the authorization. If this information is already provided in the Covered Entity’s notice given to all individuals, a reference to that notice will meet this requirement.
i. Notice of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization; and
j. Notice of the potential for information disclosed to be redisclosed by the recipient and no longer protected by the Privacy regulations.

An authorization may contain other elements which are not inconsistent with the

required elements. A valid authorization must be written in plain language.

If a Covered Entity seeks an authorization from an individual for use or disclosure of PHI, the Covered Entity must provide the individual with a copy of the signed authorization.

3. Defective Authorizations

An authorization is not valid if it has any of the following defects:

b. The expiration date has passed or the expiration event is known by the Covered Entity to have occurred;
c. The authorization has not been filled out completely with respect to a required element, if applicable;
d. The authorization is known by the Covered Entity to have been revoked;
e. The authorization is a prohibited compound or conditioned authorization;
f. 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 PHI may not be combined with any other document to create a compound authorization, except as follows:

b. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research.
c. An authorization for the use or disclosure of psychotherapy notes may only be combined with another authorization for the use or disclosure of psychotherapy notes.
d. An authorization, other than an authorization for the use or disclosure of psychotherapy notes, may be combined with any other such authorization, except where the Covered Entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations.

3. Prohibition on Conditioning 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:

b. A Covered health care provider may condition the provision of

research-related treatment on the provision of an authorization for the use or disclosure of PHI for such research;

c. A health plan may condition enrollment in the health plan or eligibility for benefits on the provision of an authorization requested by the health plan prior to enrollment, if the authorization is sought for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations and the authorization is not for a use or disclosure of psychotherapy notes.

d. A Covered Entity may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on the provision of an authorization for the disclosure of the PHI to such third party.

3. Revocation of Authorizations

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

b. The Covered Entity has taken action in reliance thereon; or

c. 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.

E. **Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object**

4. General Rule

A Covered Entity may use or disclose PHI 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 disclosure as described below. 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. Except when an objection is expressed, a Covered Entity may:

i. Use the individual's name, place within the facility, the individual's condition described in general terms, and the individual's religious affiliation to maintain a directory of individuals in its facility; and

ii. Disclose for directory purposes such information to members of the clergy or, except for religious affiliation, to other persons who ask for the individual by name.

4. Opportunity to Restrict

A covered health care provider must inform an individual of the PHI that it may include in a directory and the persons to whom it may be disclosed and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures.

4. Emergency

If the opportunity to object to uses or disclosures permitted by this section cannot be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose PHI for the facility's directory if such disclosure is:

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

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

The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes when it becomes practicable to do so.

4. Family Members

A Covered Entity may, in accordance with paragraphs (a) or (b) below, disclose to a family member, other relative or close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment for that care.

A Covered Entity may, in accordance with paragraphs (a), (b) or (c) below, disclose PHI to notify or assist in notifying a family member, personal representative or other person responsible for the care of the individual of the individual's location, general condition or death.

b. If the individual is present or otherwise available prior to the use or disclosure permitted above and has the capacity to make health care decisions, the Covered Entity may use or disclose the PHI if it obtain's the individual's agreement, it provides the individual with the opportunity to object and the individual does not express an objection, or it reasonably infers from the circumstances that the individual does not object.

b. If the individual is not present or the opportunity to object cannot practicably be provided because of incapacity or emergency, the Covered Entity may disclose only the PHI directly relevant to such person's involvement with the individual's care if the Covered Entity has determined that the disclosure is in the individual's best interest. A Covered Entity may use its professional experience and common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions,

medical supplies, X-rays and other similar forms of PHI.

b. A Covered Entity may use or disclose PHI 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 uses or disclosures of PHI to notify or assist in notifying a family member, personal representative or other person responsible for the care of the individual of the individual's location, general condition or death. The requirements of (a) and (b) apply to such uses and disclosures to the extent the Covered Entity determines they do not interfere with the ability to respond to the emergency circumstances.

B. **Uses and Disclosures for Which an Authorization or Opportunity to Agree or Object is not Required**

A Covered Entity may use or disclose PHI without the written authorization of the individual or the opportunity for the individual to agree or object in the situations described below. When the Covered Entity is required to inform the individual of, or the individual may agree to, a use or disclosure permitted below, the Covered Entity's information and the individual's agreement may be given orally.

1. Uses and Disclosures Required by Law

b. A Covered Entity may use or disclose PHI 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.

c. A Covered Entity must meet the requirements described in sections 3, 5 or 6 below for uses or disclosures required by law.

1. Uses and Disclosures for Public Health Activities

A Covered Entity may disclose PHI for the public health activities and purposes described below to:

b. 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; or at the direction of a public health authority to a foreign government agency that is acting in collaboration with a public health authority.

c. A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

d. A person subject to the jurisdiction of the FDA with respect to an FDA-regulated product or activity, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity, such as collecting or reporting adverse events, product defects or problems; to track FDA-regulated products; to enable product recalls, repairs, replacements or lookback; or to conduct post-marketing

surveillance.

e. A person who may have been exposed to a communicable disease or may 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;

f. An employer, about an individual who is member of the workforce of the employer, if:

vi. The Covered Entity is a covered health care provider who is a member of the workforce of the employer or who provides healthcare at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury.

ii The PHI that is disclosed consists of findings concerning a work-related illness or injury or workplace-related medical surveillance.

ii iThe employer needs such findings to comply with its obligations under certain federal or state laws to record such illness or injury or to carry out responsibilities for workplace medical surveillance.

iv The covered health care provider gives written notice to the individual that PHI relating to medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual when care is provided or, if care is provided at the site of the employer, by posting the notice in a prominent area where care is provided.

If the Covered Entity is also a public health authority, the Covered Entity is permitted to use PHI in all cases in which it is permitted to disclose PHI for public health activities as listed above.

3. <u>Disclosures about Victims of Abuse, Neglect or Domestic Violence</u>

Except for reports of child abuse or neglect permitted by paragraph 2(b) above, a Covered Entity may disclose PHI about an individual whom it reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority authorized by law to receive reports of such abuse, neglect, or domestic violence:

b. To the extent the disclosure is required by law and complies with and is limited according to that law;

c. If the individual agrees to the disclosure; or

d. To the extent the disclosure is expressly authorized by statute or regulation and:

vi. The Covered Entity believes the disclosure is necessary to prevent serious harm to the individuals or other potential victims; or

vii. If the individual is unable to agree due to incapacity and a law enforcement or other public official authorized to receive a report represents that the PHI to be disclosed is not intended to be used against the individual and an immediate enforcement activity depends on the disclosure and would be adversely affected by waiting.

A Covered Entity that makes a disclosure permitted above must promptly inform the individual that such a report has been made unless informing the individual would place the individual at risk of serious harm or the Covered Entity would be informing a personal representative and reasonably believes that the personal representative is responsible for the abuse, neglect or injury.

4. Uses and Disclosures for Health Oversight Activities

A Covered Entity may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, investigations, inspections, licensure or disciplinary actions, civil, administrative or criminal actions or other activities necessary for oversight of:

b. The health care system
c. Government benefit programs for which health information is relevant to beneficiary eligibility
d. Entities subject to government regulatory programs for which health information is necessary for determining compliance, or
e. Entities subject to civil rights laws for which health information is necessary for determining compliance.

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 activity does not arise out of and is not directly related to the receipt of health care, a claim for public benefits related to health or qualification for or receipt of public benefits or services when a patient's health is integral to the claim for public benefits or services. However, if the health oversight activity or investigation is in conjunction with an oversight activity or investigation related to a claim for public benefits not related to health, the joint activity is considered a health oversight activity.

If a Covered Entity is also a health oversight agency, it may use PHI for health oversight activities as permitted by this section.

4. Disclosures for Judicial and Administrative Proceedings

a. In General - A Covered Entity may disclose PHI in the course of any judicial or administrative proceeding:

i. In response to a court order; or
ii. In response to a subpoena, discovery request or other lawful

process that is not accompanied by an order of the court or administrative tribunal if:

A. The Covered Entity receives satisfactory assurance as described below from the party seeking the PHI that reasonable efforts have been made to notify the individual of the request; or

B. The Covered Entity receives satisfactory assurance as described below from the party seeking the PHI that reasonable efforts have been made to secure a qualified protective order as defined below.

b. Satisfactory Assurances of Notice - Regarding item (a)(ii)(A) above, a Covered Entity receives satisfactory assurances from a party seeking PHI if the Covered Entity receives from such party a written statement and documentation that:

i. The party has made a good faith attempt to provide written notice to the individual;

ii. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection in the court or tribunal; and

iii. The time for filing objections has lapsed and no objections were filed or all objections that were raised have been resolved by the court and disclosure is consistent with such resolution.

c. Satisfactory Assurances - Protective Order - Regarding item (a)(ii)(B) above, a Covered Entity receives satisfactory assurances from a party seeking PHI if the Covered Entity receives from such party a written statement and documentation that:

i. The parties to the dispute have agreed to a qualified protective order and have presented it to the court or tribunal; or

ii. The party seeking the PHI has requested a qualified protective order from such court or tribunal.

d. Qualified Protective Order - A qualified protective order means an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

i. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which it was requested; and

ii. Requires the return to the Covered Entity or the destruction of the PHI at the end of the litigation or proceeding.

e. Exception - Notwithstanding the above, a Covered Entity may disclose PHI in response to a subpoena, discovery request or other lawful process

that is not accompanied by an order of the court or administrative tribunal if the Covered Entity makes reasonable efforts to notify the individual of the request as specified above or the Covered Entity makes reasonable efforts to seek a qualified protective order as described above.

The provisions of this section do not supersede other provisions of this part F that otherwise permit or restrict other uses or disclosures of PHI.

6. Disclosures for Law Enforcement Purposes

A Covered Entity may disclose PHI for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (a) through (f) below are met, as applicable.

a. Pursuant to Process - A Covered Entity may disclose PHI as required by law, including laws that require reporting of certain types of wounds or injuries, except for laws regarding abuse, neglect and domestic violence subject to sections 2 and 3 above; or in compliance with and limited by:

   i. A court order, warrant, subpoena or summons issued by a judge;
   ii. A grand jury subpoena;
   iii. An administrative request, subpoena, summons, a civil investigative demand, or similar process authorized by law, provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope, and de-identified information could not reasonably be used.

b. Identification and Location Purposes - Except for disclosures required by law as permitted by (a) above, a Covered Entity may disclose PHI to a law enforcement official for the purpose of identifying a suspect, fugitive, material witness or missing person, provided that it may disclose only the following information: name and address; date and place of birth; social security number; blood type; type of injury; date and time of treatment; date and time of death, if applicable; and a description of distinguishing characteristics.

   Except for the information listed above, a Covered Entity may not disclose for the purposes of identification or location any PHI related to an individual's DNA, dental records, or typing, samples or analysis of body fluids or tissue.

c. Victims of a Crime - Except for disclosures required by law as permitted by (a) above, a Covered Entity may disclose PHI to a law enforcement official about an individual who is suspected of being a victim of a crime, other than disclosures subject to sections 2 and 3 above, if the individual agrees to the disclosure, or the Covered Entity is unable to obtain the

individual's agreement due to incapacity or emergency, provided that:

i. The law enforcement official represents such PHI is needed to determine whether another person violated the law and such information is not intended to be used against the victim;
ii. The law enforcement official represents that immediate law enforcement activity depends on the disclosure and would be materially and adversely affected by waiting; and
iii. The Covered Entity determines the disclosure is in the best interests of the individual.

d. Decedents - A Covered Entity may disclose PHI about a person who has died to a law enforcement official for the purpose of alerting law enforcement of the death if the Covered Entity has a suspicion that the death resulted from criminal conduct.

e. Crime on Premises - A Covered Entity may disclose to a law enforcement official PHI that the Covered Entity believes in good faith constitutes evidence that a crime occurred on the premises of the Covered Entity.

f. Reporting Crime in Emergencies - A covered health care provider providing emergency health care off the premises of the covered health care provider may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to the commission and nature of a crime, the location of such crime or victim of such crime, and the identity, description and location of the perpetrator of such crime. If a covered health care provider believes that such emergency is the result of abuse, neglect or domestic violence, this paragraph does not apply and the disclosure is subject to section 3 above.

6. Uses and Disclosures about Decedents

a. Coroners and Medical Examiners - A Covered Entity may disclose PHI 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 PHI for these purposes.

b. Funeral Directors - A Covered Entity may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent.

6. Uses and Disclosures for Organ, Eye or Tissue Donation Purposes

A Covered Entity may use or disclose PHI to organ procurement organizations or other

entities engaged in procurement, banking or transplantation of organs, eyes or tissue for the purpose of facilitating donation and transplantation.

6. Uses and Disclosures for Research Purposes

a. In General - A Covered Entity may use or disclose PHI for research, regardless of the source of funding of the research, provided that:

i. The Covered Entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization for use or disclosure of PHI has been approved by either:

A. An IRB; or
B. A privacy board that has members of varying backgrounds and appropriate professional competency to review the effect of the research; includes at least one member not affiliated with the Covered Entity, any sponsor of the research or any affiliate of either; and does not have any member participating who has a conflict of interest

ii. The Covered Entity obtains from the researcher representations that:

A. Use or disclosure is sought solely to review PHI a necessary to prepare a research protocol or for similar purposes preparatory to research;
B. No PHI is to be removed from the Covered Entity; and
C. The PHI is necessary for the research purposes.

iii. The Covered Entity obtains from the researcher:

A. Representation that the use or disclosure sought is solely for research on the PHI of decedents;
B. Documentation at the request of the Covered Entity of the death of such individuals; and
C. Representation that the PHI is necessary for the research purposes.

b. Documentation of Waiver - For a use or disclosure to be permitted based upon documentation of approval of an alteration or waiver of authorization, the documentation must include all of the following:

i. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;
ii. 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 PHI involved 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 use and disclosure;
    2. A adequate plan to destroy the identifiers at the earliest opportunity consistent with the 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 PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure would be permitted by the regulations;
B. The research could not practicably be conducted without the waiver or alteration; and
C. The research could not practicably be conducted without access to and use of the PHI.

iii. A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board;

iv. 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;
B. A privacy board must review the proposed research at convened meetings at which a majority of the board members are present, including one not affiliated with the Covered Entity, any sponsor of the research or any affiliate of either, and the alteration or waiver of authorization must be approved by a majority of the board present at the meeting, unless the board elects to use an expedited review procedure;
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 PHI. If the 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 board, or by one or more members as designated by the chair; and

v. 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 privacy board, as applicable.

10. Uses and Disclosures to Avert a Serious Threat to Health or Safety

a. Permitted Disclosures - A Covered Entity may, consistent with applicable law and ethical standards, use or disclose PHI, if the Covered Entity in good faith believes the use or disclosure:

i. Is necessary to lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;
ii. Is necessary for law enforcement authorities to identify or apprehend an individual who has admitted participating in a violent crime that may have caused serious physical harm to the victim or where it appears the individual has escaped from a correctional institution or lawful custody.

b. Use or Disclosure not Permitted - A use or disclosure to law enforcement authorities to identify or apprehend an individual who has admitted participating in a violent crime that may have caused serious physical harm to the victim may not be made if the information is learned by the Covered Entity

i. In the course of treatment to affect the propensity to commit the criminal conduct which is the basis for the disclosure, or counseling or therapy; or
ii. Through a request by the individual to initiate or be referred for such treatment, counseling or therapy.

c. Limit on What May Be Disclosed - A disclosure to law enforcement authorities to identify or apprehend an individual who has admitted participating in a violent crime that may have caused serious physical harm to the victim may only include the statement of admission and the PHI described in section 6(b) above.

d. Presumption of Good Faith - A Covered Entity that uses or discloses PHI pursuant to paragraph (a) above is presumed to have acted in good faith with regard to a belief described in paragraph (a) above if the belief is

based on the Covered Entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

11. Uses and Disclosures for Specialized Government Functions

a. Armed Forces Personnel - A Covered Entity may use and disclose PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command to assure proper execution of the military mission, if the appropriate military authority has published in the Federal Register the following information:

i. Appropriate military command authorities; and
ii. The purposes for which the PHI may be used or disclosed.

b. Separation or Discharge - A Covered Entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the PHI 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 determining eligibility for DVA benefits.

c. Veterans - A Covered Entity that is a component of the Department of Veterans Affairs may use and disclose PHI to components of the Department that determine eligibility for or entitlement to, or that provide, DVA benefits.

d. Foreign Military Personnel - A Covered Entity may use and disclose PHI 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 under paragraph (a) above.

e. National Security and Intelligence - A Covered Entity may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence and authorized national security activities.

f. Protective Services - A Covered Entity may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by law, or to foreign heads of state or other persons, or to conduct investigations authorized by 18 U.S.C. 871 and 879.

g. Medical Suitability Determinations - A Covered Entity that is a component of the Department of State may use PHI 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;
ii. As necessary to determine worldwide availability or availability for mandatory service abroad under the Foreign Service Act; or
iii. For a family to accompany a Foreign Service member abroad consistent with the Foreign Service Act.

h. Correctional Institutions and Law Enforcement Custody - A Covered Entity may disclose to a correctional institution or a law enforcement official having lawful custody of an individual PHI of that individual if the correctional institution or official represents that such PHI is necessary for:

i. The provision of health care to the individual;
ii. The health and safety of such individual or other inmates;
iii. The health and safety of the officers or employees or others at the correctional institution;
iv. The health and safety of such individuals and officers or others responsible for transporting or transferring inmates;
v. Law enforcement on the premises of the correctional institution; and
vi. The administration and maintenance of the safety, security and good order of the correctional institution.

A Covered Entity that is a correctional institution may use PHI of inmates for any purpose for which such PHI may be disclosed.

An individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

i. Government Programs Providing Benefits - A health plan that is a government program providing public benefits may disclose PHI relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of such PHI in a data system is required or expressly authorized by statute or regulation.
A Covered Entity that is a government agency administering a government program providing public benefits may disclose PHI 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 PHI is necessary to coordinate covered functions or to improve administration of such programs.

12. Disclosures for Workers' Compensation

A Covered Entity may disclose PHI 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.

G. Other Requirements Relating to Uses and Disclosures of PHI

1. De-Identification

Health Information which does not identify an individual and with respect to which there is no reasonable basis to believe the information can be used to identify an individual is not individually identifiable health information. A Covered Entity may determine that health information is not individually identifiable health information only if:

a. A person with appropriate knowledge and experience, applying generally accepted statistical and scientific principles and methods, determines the risk is very small that the information could be used alone or in combination with reasonably available information by a recipient to identify the individual who is the subject of the information; and that person documents the methods and results of the analysis that justify such determination; or

b. The following identifiers of the individual or of relatives, employers or household members of the individual, are removed:

vi. Names;
vii. All geographic subdivisions smaller than a State, except for the initial three digits of a zip code in certain circumstances;
viii. All elements of dates except year and all ages over 89;
ix. Telephone numbers;
x. Fax numbers;
xi. Electronic mail addresses;
xii. Social security numbers;
xiii. Medical record numbers;
xiv. Health plan beneficiary numbers;
xv. Account numbers;
xvi. Vehicle identifiers, serial and license plate numbers;
xvii. Device identifiers and serial numbers;
xviii. URL's;
xix. IP address numbers;
xx. Biometric identifiers, including finger and voice prints;
xxi. Full-face photographs and comparable images; and
xxii. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) below.
xviii. Certificate/license numbers;

c. A Covered Entity may assign a code or other means of record identification to allow de-identified information to be re-identified by the Covered Entity, provided that:

i. The code or other means is not derived from or related to information about the individual and is not otherwise capable of being translated to identify the individual; and

ii. The Covered Entity does not use or disclose the code or other means for any other purpose and does not disclose the mechanism for re-identification.

2. Minimum Necessary Requirements

A Covered Entity must meet the following requirements with respect to a request for, or the use and disclosure of PHI.

a. Uses of PHI - A Covered Entity must:

i. Identify the persons or classes of persons in its workforce who need access to PHI to carry out their duties;

ii For each such person or classes of persons, identify the category or categories of PHI to which access is needed and any conditions appropriate to such access; and

iii. Limit the access of such persons or classes identified in (i) to the PHI identified in (ii).

b. Disclosures of PHI

i. For routine and recurring disclosures, a Covered Entity must implement policies and procedures that limit the PHI 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 PHI disclosed to the information reasonably necessary to accomplish the purpose of the disclosure; and

B. Review requests for disclosure on an individual basis in accordance with such criteria.

i. A Covered Entity may rely, if such reliance is reasonable, on a requested disclosure as the minimum necessary for the stated purpose when:

A. Making permitted disclosures to public officials if the public official represents that the information requested is the minimum necessary;

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 a Business Associate for the

purpose of providing professional services to the Covered Entity and the professional represents that the information requested is the minimum necessary; or

D. Documentation or representations complying with the requirements pertaining to research have been providing by a person requesting the information for research purposes.

c. Requests for PHI

vi. When requesting PHI from other Covered Entities, a Covered Entity must limit its request to that which is reasonably necessary to accomplish the purpose for which the request is made.

vii. For routine and recurring requests, a Covered Entity must implement policies and procedures that limit the PHI requested to the amount reasonably necessary to achieve the purpose for which the request is made.

viii. For all other requests, a Covered Entity must:

A. Develop criteria designed to limit the request for PHI 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.

d. Entire Record - For all uses, disclosures or requests to which the minimum necessary requirements apply, a Covered Entity may not use, disclose or request an entire medical record, except when the entire medical record is the amount reasonably necessary to accomplish the purpose.

3. Limited Data Set

A Covered Entity may use or disclose a limited data set that meets the requirements of this section, if the Covered Entity enters into a data use agreement with the limited data set recipient.

a. Definition - A limited Date set is PHI 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. Medical record numbers;

viii. Health plan beneficiary numbers;
ix. Account numbers;
x. Certificate/license numbers;
xi. Vehicle identifiers, serial and license plate numbers;
xii. Device identifiers and serial numbers;
xiii. URL's;
xiv. IP address numbers;
xv. Biometric identifiers, including finger and voice prints; and
xvi. Full-face photographs and comparable images.

b. Permitted Purposes

i. A Covered entity may use or disclose a limited data set only for the purposes of research, public health, or health care operations.
ii. A Covered Entity may use PHI to create a limited data set, or disclose PHI only to a business associate for such purpose, whether or not the limited data set is to be used by the Covered Entity.

c. Data Use Agreement

A Covered Entity may use or disclose a limited data set only if the Covered Entity obtains a data use agreement that meets the requirements of this section. A data use agreement between the Covered Entity and the limited data set recipient must:

vi. Establish the permitted uses and disclosures of such information by the recipient. The agreement may not authorize the recipient to use or further disclose the information in a manner that would violate the requirements of the Privacy regulations if done by the Covered Entity;
vii. Establish who is permitted to use or receive the limited data set;
viii. Provide that the recipient will:
A. Not use or further disclose the information other than as permitted by the agreement or required by law;
B. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the agreement;
C. Report to the Covered Entity any use or disclosure of the information not provided for in the agreement of which it becomes aware;
D. Ensure that any agents to whom it provides the limited data set agrees to the same restrictions and conditions as the recipient; and
E. Not identify the information or contact the individuals.

A Covered Entity is not in compliance if it knew of a pattern of activity of the 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 and, if such steps were unsuccessful, discontinued disclosure of PHI to the recipient and reported the problem to the Secretary of DHHS. A Covered Entity that is a limited data set recipient and violates a data use agreement will be in violation of the requirements of this section.

4. Fund raising

a. In General - A Covered Entity may use, or disclose to a business associate or to an institutionally related foundation, the following PHI for the purposes of raising funds for its own benefit, without an authorization:
   i. Demographic information; and
   ii. Dates of health care provided to an individual.

b. Requirements

i. The Covered Entity may not use or disclose PHI for fund raising purposes unless a statement is included in the notice provided to individuals by the Covered Entity.

ii. The Covered Entity must include in fund raising materials it sends to an individual a description of how the individual may opt out of receiving any further fund raising communications.

iii. The Covered Entity must make reasonable efforts to ensure that individuals who opt out are not sent such communications.

5. Underwriting - If a health plan receives PHI 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 PHI for any other purpose, except as required by law.

6. Verification Requirements

a. General - Prior to any permitted disclosure, a Covered Entity must:
   i. Except with respect to uses and disclosures requiring an opportunity for the individual to agree or object, verify the identity of a person requesting PHI and the authority of the person to have access to PHI, if the identity or authority are not known to the Covered Entity; and
   ii. Obtain any documentation, statements, or representations, from the

person requesting PHI when such documentation, statement or representation is a condition of disclosure.

b. Conditions - If disclosure is conditioned on particular documentation, statements, or representations from the person requesting PHI, a Covered Entity may rely, if such reliance is reasonable, on documentation, statements or representations that on their face meet the applicable requirements.

c. Identity of Public Officials - A Covered Entity may rely, if such reliance is reasonable, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:
   i. If the request is made in person, presentation of an agency badge, credentials or other proof of government status;
   ii. If the request is in writing, the request is on appropriate government letterhead; or
   iii. If the disclosure is to a person acting on behalf of the 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 that establishes that the person is acting on behalf of the public official.

d. Authority of Public Officials - A Covered Entity may rely, if such reliance is reasonable, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:
   i. A written statement of the legal authority under which the information is requested or, if a written statement is impracticable, an oral statement of such legal authority;
   ii. 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.

e. Good Faith - The verification requirements are met if the Covered Entity relies on the exercise of professional judgment in making a use or disclosure in accordance with the requirements for uses and disclosures requiring an opportunity for the individual to agree or object or acts on a good faith belief in making a disclosure in accordance with the requirements for uses and disclosures for which an authorization or opportunity to agree or object is not required.

H. Notice of Privacy Practices for PHI

1. General - Except as provided in this section, an individual has a right to adequate notice of the uses and disclosures of PHI that may be made by a

Covered Entity, and of the individual's rights and the Covered Entity's legal duties with respect to PHI.

2. Exception for Group Health Plans - An individual 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.
   c. A group health plan that provides benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives PHI in addition to summary information, participation information or enrollment information, must maintain a notice and provide such notice upon request to any person. The provisions of paragraph 4(a) below do not apply to such health plans.
   d. A group health plan that provides benefits solely through an insurance contract with a health insurance issuer or HMO, and that does not create or receive PHI other than summary information, participation information or enrollment information, is not required to maintain or provide a notice under this section.
3. Content of Notice - The Covered Entity must provide a notice that is written in plain language and that contains the following elements:
   a. Header - "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."
   b. Uses and Disclosures - The notice must contain:
      i. A description, including at least one example, of permitted uses and disclosures for each of the following purposes: treatment, payment and health care operations.
      ii. A description of each of the other purposes for which use or disclosure without the individual's authorization is permitted or required.
      iii. If any use or disclosure described in (A) or (B) is prohibited or materially limited by other applicable law, the description must reflect the more stringent law.
      iv. The descriptions must be sufficiently detailed to put the individual on notice of the permitted and required uses and disclosures.
      v. 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.

b. Special Uses and Disclosures - If the Covered Entity intends to engage in any of the following activities, the description of uses and disclosures must include a separate statement, as applicable, that:

i. The Covered Entity may contact the individual to provide appointment reminders or information about treatment or services which may be of interest to the individual.

ii. The Covered Entity may contact the individual to raise funds for the Covered Entity; or

iii. A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose PHI to the sponsor of the plan.

b. Individual Rights - The Notice must contain a statement of the individual's rights with respect to PHI and a brief description of how the individual may exercise these rights, as follows:

i. The right to request restrictions on certain uses and disclosures, and that the Covered Entity is not required to agree to a requested restriction;

ii. The right to receive confidential communications of PHI;

iii. The right to inspect and copy PHI;

iv. The right to amend PHI;

v. The right to receive an accounting of disclosures; and

vi. The right of an individual, including an individual who has agreed to receive the notice electronically, to obtain a paper copy of the notice upon request.

b. Covered Entity's Duties - The Notice must contain:

i. A statement that the Covered Entity is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices;

ii. A statement that the Covered Entity is required to abide by the terms of the notice currently in effect; and

iii. To apply a change in a privacy practice described in the notice to PHI created or received prior to issuing a revised notice , a statement that the Covered Entity reserves the right to change the terms of the notice and to make new notice provisions effective for all PHI that it maintains. The statement must also state how it will provide individuals with a revised notice.

b. Complaints - The notice must contain a statement that individuals may complain to the Covered Entity and to the Secretary of DHHS if they believe their privacy rights have been violated, how to make a complaint with the Covered Entity and a statement that the individual will not be retaliated against for

making a complaint.

c. Contact - The notice must contain the name or title, and telephone number of the person or office to contact for further information.

d. 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.

e. Revisions - 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 in the notice. Except when required by law, a material change may not be implemented prior to the effective date in the notice in which such change is reflected.

4. Provision of Notice - A Covered Entity must make the notice available on request to any person and to individuals, as follows:

a. Health Plans - A health plan must provide notice:

i. No later than the compliance date for the health plan to individuals then covered by the plan;

ii. Thereafter, at the time of enrollment for new enrollees; and

iii. Within 60 days of a material revision to the notice to individuals then covered by the plan.

iv. 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.

v. The health plan satisfies the notice requirements of this subsection 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.

vi. If a health plan has more than one notice, it satisfies the requirements of this subsection by providing the notice that is relevant to the individual or other person requesting the notice.

b. Certain Health Care Providers - A covered health care provider that has a direct treatment relationship with an individual must:

i. Provide the notice no later than the date of first service delivery, including service delivered electronically, after the compliance date for the provider or, in the case of emergency treatment, as soon as practicable after the emergency treatment.

ii. Except in emergency treatment situations, make a good faith effort to obtain a written acknowledgment of receipt of the notice, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason it was not obtained.

iii. If the provider maintains a physical service delivery site, have the notice available at the site for individuals to request and take with them and post the notice in a clear and prominent location for individuals to be able to read.

iv. When the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with subsection (iii) above.

c. Electronic Notice

i. A Covered Entity that maintains a web site that provides information about the provider's services or benefits must prominently post the notice on the web site and make it electronically available through the web site.

ii. A Covered Entity may provide the notice by e-mail if the individual has agreed to electronic notice and such agreement has not been withdrawn. If the Covered Entity knows the e-mail transmission has failed, it must provide a paper copy.

iii. If the first service delivery is electronic, the provider must provide electronic notice automatically and at the same time as the individual's first request for service. The requirements regarding obtaining an acknowledgment of receipt of the notice apply to electronic notice.

iv. The individual who receives electronic notice retains the right to obtain a paper copy upon request.

d. Joint Notice by Separate Entities - Covered Entities that participate in an OHCA may comply with the notice requirements by a joint notice provided that specific requirements are met.

e. Documentation - A Covered Entity must document compliance with the notice requirements 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.

I. Rights to Request Privacy Protection for PHI

1. Right of Individual to Request Restriction of Uses and Disclosures

a. A Covered Entity must permit an individual to request that the Covered Entity restrict uses or disclosures of PHI for treatment, payment or health care operations, and disclosures for involvement in the individual's care and notification purposes.

b. A Covered Entity is not required to agree to a restriction.

c. A Covered Entity that agrees to a restriction may not use or disclose PHI in violation of the restriction except that, where the restricted PHI is needed for emergency treatment, the Covered Entity may use or disclose such PHI to a health care provider to

provide such treatment to the individual. If the restricted PHI is disclosed for emergency treatment, the Covered Entity must request that the health care provider not further use or disclose the information.

d. A restriction agreed to is not effective to prevent uses or disclosures permitted or required to the Secretary of DHHS for compliance, for facility directories or for which authorization or an opportunity to agree or object is not required.

e. Terminating a Restriction - A Covered Entity may terminate its agreement to a restriction if:

iii. The individual agrees to or requests the termination in writing;

iv. The individual orally agrees to the termination and the oral agreement is documented; or

v. The Covered Entity informs the individual it is terminating its agreement to the restriction, except that such termination is only effective with regard to PHI created or received after it has so informed the individual.

f. A Covered Entity that agrees to a restriction must document that restriction.

2. Confidential Communications Requirements

a. A covered health care provider must permit individuals to request and must accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations.

b. A health plan must permit individuals to request and must accommodate reasonable requests to receive communications of PHI 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.

c. A Covered Entity may require an individual to make a request for a confidential communication in writing.

d. A Covered Entity may condition the provision of a reasonable accommodation on information as to how payment, if any and when appropriate, will be handled and specification of an alternative address or other method of contact. A Covered Entity may not require an explanation of the basis for the request as a condition.

J. Access of Individuals to PHI

1. Access to PHI

a. Right of Access - Except as otherwise provided in this section, an individual has a right of access to inspect and obtain a copy of PHI

about the individual in a designated record set, for as long as the PHI is maintained in the record, 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. PHI that is maintained by a Covered Entity that is subject to the Clinical Laboratory Improvements Amendments of 1988, to the extent provision of access would be prohibited by law, or is exempt from the CLIA.

b. Unreviewable Grounds for Denial - A Covered Entity may deny an individual access without providing the individual an opportunity to review, in the following circumstances:

i. The PHI is excepted from the right of access by paragraph (a) above;
ii. A Covered Entity that is a correctional institution or a covered health care provider acting under the direction of a correctional institution may deny an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, custody or rehabilitation of the inmate or others.
iii. Access to PHI created or obtained by a health care provider in the course of research that includes treatment may be temporarily suspended while the research is in progress, provided the individual has agreed to the denial of access when consenting to participate and the health care provider has informed the individual that access will be reinstated upon completion of the research.
iv. An individual's access to PHI in records subject to the Privacy Act 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 PHI was obtained from someone other than a health care provider under a promise of confidentiality and access would likely reveal the source of the information.

c. Reviewable Grounds for Denial - A Covered Entity may deny an individual access, provided the individual is given a right to have the denial reviewed, in the following circumstances:

i. A licensed health care professional has determined that the access requested is likely to endanger the life or physical safety of the individual or another person;
ii. The PHI makes reference to another person, (other than a health care provider) and a licensed health care professional has determined that the access requested is likely to cause substantial harm to the other person; or
iii. The request for access is made by the individual's personal

representative and a licensed health care professional has determined that the provision of access to the personal representative is likely to cause substantial harm to the individual or another person.

d. Review of a Denial of Access - If access is denied under paragraph (c), the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Covered Entity 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 decision of the reviewing official.

2. Requests for Access and Timely Action

a. Requests for Access - The Covered Entity must permit an individual to request access to inspect or obtain a copy of PHI about the individual in a designated record set. The Covered Entity may require individuals to make requests for access in writing, provided it informs individuals of such a requirement.

b. Timely Action by the Covered Entity

i. Except as provided in subsection (ii) below, the Covered Entity must act on a request for access no later than 30 days after receipt of the request by either informing the individual of the acceptance of the request and providing the access requested or providing a written denial of the request.

ii. If the request is for PHI that is not maintained or accessible to the Covered Entity on-site, the Covered Entity must take an action required under subsection (i) no later than 60 days from the receipt of the request.

iii. If the Covered Entity is unable to take action within the time required, the Covered Entity may extend the time for such actions by no more than 30 days, provided that it provides a written statement to the individual within the original time limit stating the reasons for the delay and the date by which it will complete its action, and the Covered Entity may have only one such extension.

3. Provision of Access - If the Covered Entity provides an individual with access to PHI, the Covered Entity must comply with the following requirements:

a. Providing the Access Requested - The Covered Entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the PHI about the individual in a designated record set. If the same PHI is maintained in more than one record set or location, the Covered Entity need only produce the PHI once in response to a request.

b. Form of Access Requested

i. The Covered Entity must provide the access in the form or

format requested by the individual, if readily producible, or, if not, in a readable hard copy or other format as agreed to by the Covered Entity and the individual.

ii. The Covered Entity may provide a summary of the PHI in lieu of providing access or may provide an explanation of the PHI requested, if the individual agrees in advance to such a summary or explanation and the individual agrees in advance to any fees imposed for such summary or explanation.

c. Time and Manner of Access - The Covered Entity must provide access in a timely manner, including arranging for a convenient time and place for the individual to inspect or obtain a copy of the PHI or mailing a copy at the individual's request. The Covered Entity may discuss the aspects of the request to facilitate timely access.

d. Fees - If the individual requests a copy of the PHI or agrees to a summary or explanation, the Covered Entity may impose a reasonable, cost-based fee, provided the fee includes only the cost of:

i. Copying, including the cost of supplies and labor;

ii. Postage, when the individual has requested the copy be mailed; and

iii. Preparing an explanation or summary of the PHI, if agreed to by the individual.

4. Denial of Access - If a Covered Entity denies access, in whole or in part, to PHI, the Covered Entity must comply with the following requirements:

a. Making Information Accessible - The Covered Entity must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which the Covered Entity has a ground to deny access.

b. Denial - The Covered Entity must provide a timely, written denial to the individual. The denial must be in plain language and contain:

i. The basis for the denial;

ii. If applicable, a statement of the review rights, including a description of how to exercise such review rights: and

iii. A description of how the individual may complain to the Covered Entity or to the Secretary of DHHS. The description must include the name, or title, and phone number of the designated contact person or office.

c. Other Responsibility - If the Covered Entity does not maintain the PHI requested, and the Covered Entity knows where the PHI is maintained, the Covered Entity must inform the individual where to direct the request for access.

d. Review of Denial Requested - If the individual has requested a review of the denial, the Covered Entity must designate a licensed

health care professional, who did not participate in the original decision to deny, to review the decision to deny and must promptly refer the request for review to such designated reviewing official. The designated reviewing official must determine within a reasonable time whether or not to deny access. The Covered Entity must promptly provide written notice to the individual of the decision of the designated reviewing official and provide or deny access in accordance with that decision.

5. Documentation - A Covered Entity must document the following and retain the documentation as required by the regulations:
   a. The designated record sets that are subject to access by individuals; and
   b. The titles of persons or offices responsible for receiving and processing requests for access by individuals.

K. Amendment of PHI

1. Right to Amend
   a. Right to Amend - An individual has the right to have a Covered Entity amend PHI or a record about an individual in a designated record set for as long as the PHI is maintained in the designated record set.
   b. Denial of Amendment - A Covered Entity may deny a individual's request for amendment if it determines that the PHI 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 the originator of the PHI 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 the right to request access; or
      iv. Is accurate and complete.
2. Requests for Amendment and Timely Action
   a. Request for Amendment - The Covered Entity must permit an individual to request that the Covered Entity amend the PHI maintained in the designated record set. The Covered Entity may require that such requests be in writing and provide a reason to support the requested amendment, provided it informs individuals of such requirements in advance.
   b. Timely Action by the Covered Entity - The Covered Entity must act on a request for amendment no later than 60 days after receipt of the request, as follows:
      i. If it grants the request, in whole or in part, it must take the actions required by section (3) below.
      ii. If it denies the requested amendment, in whole or in part, it

must provide a written denial.

iii. If it is unable to act within the time required, the Covered Entity may extend the time for such action by no more than 30 days, provided that it provides a written statement to the individual within the original time limit stating the reasons for the delay and the date by which it will complete its action, and the Covered Entity may have only one such extension.

3. 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:
   a. Making the Amendment - The Covered Entity must make the appropriate amendment to the PHI or record by, at a minimum, identifying the records affected by the amendment and appending or otherwise linking to the amendment.
   b. Informing the Individual - 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.
   c. 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 the PHI and needing the amendment; and
      ii. Persons, including business associates, that the Covered Entity knows have the PHI 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.
4. 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.
   a. Denial - The Covered Entity must provide the individual with a timely, written denial. The denial must use plain language and contain:
      i. The basis for the denial;
      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 the Covered Entity provide the individual's request for amendment and the denial with any future disclosures of the PHI; and
      iv. A description of how the individual may complain to the

Covered Entity or to the Secretary of DHHS. The description must include the name, or title, and phone number of the designated contact person or office.

b. Statement of Disagreement - The Covered Entity must permit the individual to submit a written statement disagreeing with the denial of all or part of the amendment and the basis of such disagreement. The Covered Entity may reasonably limit the length of a statement of disagreement.

c. Rebuttal Statement - The Covered Entity may prepare a written rebuttal to the statement of disagreement. Whenever a rebuttal is prepared, a copy must be provided to the individual.

d. Recordkeeping - The Covered Entity must, as appropriate, identify the record of PHI that is the subject of the disputed amendment and append or otherwise link the request, the denial, the statement of disagreement and the rebuttal to the designated record set.

e. Future Disclosures

i. If a statement of disagreement has been submitted, the Covered Entity must include the information appended to the record, or an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates.

ii. If the individual has not submitted a statement of disagreement, the Covered Entity must include the request for amendment and the denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.

iii. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the Covered Entity may separately transmit the material required to be sent, to the recipient of the standard transaction.

5. Actions on Notices of Amendment - A Covered Entity that is informed by another Covered Entity of an amendment to an individual's PHI, must amend the PHI in designated record sets.

6. 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 the regulations.

L. Accounting of Disclosures of PHI

1. Right to an Accounting of Disclosures of PHI

a. Right to an Accounting - An individual has right to receive an accounting of disclosures of PHI 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;
ii. To individuals of PHI about them;
iii. Incident to a use or disclosure otherwise permitted or required;
iv. Pursuant to an authorization;
v. For the facility's directory or to persons involved in the individual's care or other notification purposes;
vi. For national security or intelligence purposes;
vii. To correctional institutions or law enforcement officials in custodial situations;
viii. As part of a limited data set; or
ix. That occurred prior to the compliance date for the Covered Entity.

b. Suspension of Right to an Accounting - The Covered Entity must suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides a written statement that such an accounting would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
   i. If the agency or official statement 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; and
      C. Limit the temporary suspension no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

c. Time Period - An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

2. Content of the Accounting - The Covered Entity must provide the individual with a written accounting that meets the following requirements:
   a. Except as otherwise provided in section (1) above, the accounting must include disclosures of PHI that occurred during the six years (or a shorter period of time at the request of the individual) prior to the date of the request, including disclosures to or by business associates of the Covered Entity.
   b. Except as otherwise provided by paragraphs (c) and (d) below, the accounting must include for each disclosure:
      i. The date of the disclosure;
      ii. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

iii. A brief description of the PHI disclosed; and
iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for a disclosure, if any.

c. If, during the period covered by an accounting, the Covered Entity has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:
i. The information required by paragraph (b) above 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 disclosure during the accounting period.

d. If, during the period covered by the accounting, the Covered Entity has made disclosures of PHI for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosures for which PHI of the individual may have been included, provide:
i. The name of the protocol or other research activity;
ii. A description in plain language of the research protocol or activity, including the purpose and criteria for selecting particular records;
iii. A brief description of the type of PHI disclosed;
iv. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
v. The name, address and telephone number of the entity that sponsored the research and of the researcher to whom the PHI was disclosed; and
vi. A statement that the PHI may or may not have been disclosed for a particular protocol or other research activity.

If the Covered Entity provides an accounting for research disclosures in accordance with this section, and if it is reasonably likely that the PHI of the individual was disclosed for such research, the Covered Entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

3. <u>Provision of the Accounting</u>

a. The Covered Entity must act on an 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 accounting requested: or
ii. If the Covered Entity is unable to provide the accounting within the time required, the Covered Entity may extend

the time for such action by no more than 30 days, provided that it provides a written statement to the individual within the original time limit stating the reasons for the delay and the date by which it will provide the accounting, and the Covered Entity may have only one such extension.

b. 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 opportunity to withdraw or modify the request in order to avoid or reduce the fee.

4. Documentation - A Covered Entity must document the following and retain the documentation as required by the regulations:
   a. The information required to be included in an accounting for disclosures of PHI that are subject to an accounting;
   b. The written accounting that is provided to an individual; and
   c. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

M. Administrative Requirements

1. Personnel Designations
   a. A Covered Entity must designate a privacy official who is responsible for the development and implementation of policies and procedures of the entity and a contact person or office who is responsible for receiving complaints and who is able to provide further information about matters covered in the notice provided to individuals.
   b. A Covered Entity must document such personnel designations as required by subsection (10) of this section.
2. Training
   a. A Covered Entity must train all members of its workforce on the policies and procedures with respect to PHI, as necessary and appropriate for the members of the workforce to carry out their function within the Covered Entity.
   b. A Covered Entity must provide training as follows:
      i. To each member of its workforce by no later than the compliance date;
      ii. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the workforce; and to each member of its workforce whose functions are affected by a material change in the policies or procedures, within a reasonable period of time after the change becomes effective.
      iii. A Covered Entity must document that the required training

has been provided as required by subsection (10) of this section.

3. Safeguards
   a. A Covered Entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI.
   b. A Covered Entity must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the regulations.
   c. A Covered Entity must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.
4. Complaints to the Covered Entity
   a. A Covered Entity must provide a process for individuals to make complaints concerning its policies and procedures or its compliance with such policies and procedures or the requirements of these regulations.
   b. A Covered Entity must document all complaints received and their disposition, if any.
5. Sanctions
   a. A Covered Entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the policies and procedures or the requirements of the regulations. This standard does not apply to members of the workforce who are whistleblowers, victims of crime or who have filed a complaint, participated in an investigation or opposed an unlawful act or practice.
   b. A Covered Entity must document any sanctions that are applied.
6. 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 PHI in violation of its policies and procedures or the requirements of these regulations by the Covered Entity or its business associate.
7. Refraining from Intimidation or Retaliatory Acts - A Covered Entity may not intimidate, threaten, coerce, discriminate against, or take retaliatory action against:
   a. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established under the regulations, including the filing of a complaint.
   b. Any individual or other person:
      i. Filing a complaint with the Secretary of DHHS;
      ii. Testifying, assisting, or participating in an investigation, compliance review or hearing; or
      iii. Opposing any act or practice made unlawful by the regulations, provided the person has a good faith belief that the practice opposed is unlawful, and the manner of the

opposition is reasonable and does not involve disclosure of PHI in violation of the regulations.

8. Waiver of Rights - A Covered Entity may not require individuals to waive their rights to file complaints or other rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

9. Policies and Procedures

   a. General - A Covered Entity must implement policies and procedures with respect to PHI that are designed to comply with the standards and requirements of the regulations. The policies and procedures must be reasonably designed, considering the size and activities related to PHI of the Covered Entity, to ensure compliance.

   b. Changes to Policies and Procedures

      i. A Covered Entity must change its policies and procedures as necessary and appropriate to comply with changes in the law and regulations.

      ii. When a Covered Entity changes a privacy practice that is stated in the notice, and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI created or received prior to the effective date of the notice revision if it has 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 subsection (e) below.

   c. Changes in Law - Whenever there is a change in law that necessitates a change to its policies or procedures, it must promptly document and implement the revised policy or procedure. If the change in law materially affects its notice, the Covered Entity must promptly make the appropriate revisions to the notice. Nothing in this paragraph may be used to excuse a failure to comply with the law.

   d. Changes to Privacy Practices Stated in the Notice

      i. To implement a change in its policies and procedures to reflect a change in a privacy practice that is stated in its notice, a Covered Entity must:

         A. Ensure that the policy or procedure, as revised to reflect a change in a privacy practice that is stated in its notice, complies with the regulations;

         B. Document the policy or procedure, as revised, as required by subsection 10; and

         C. Revise the notice as required to state the changed practice and make the revised notice available as

required. 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 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 PHI 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 subsection (d)(i)(A)-(C) above; and

B. Such change is effective only with respect to PHI created or received after the effective date of the notice.

e. Changes to Other Policies and Procedures - A Covered Entity may change, at any time, a policy or procedure that does not materially affect the content of the notice, provided that:

i. The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of the regulations; and

ii. Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by subsection (10) below.

10. Documentation - A Covered Entity must:

a. Maintain the policies and procedures provided for in subsection (9) above in written or electronic form;

b. If a communication is required by the regulations to be in writing, maintain such writing, or an electronic copy, as documentation; and

c. If an action, activity, or designation is required by the regulations to be documented, maintain a written or electronic record of such action, activity or designation; and

d. Retain the documentation required by this paragraph for six years from the date of its creation or the date when it was last in effect, whichever is later.

11. Group Health Plans

a. A group health plan is not subject to the standards or implementation specifications in subsections (1) through (6) and (9) of this section, to the extent that:

i. The group health plan provides 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 PHI, except for:
A. Summary health information; 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.

b. A group health plan described in paragraph (11)(a) above is subject to the standard and implementation specification in paragraph (10) of this subsection only with respect to plan documents amended in accordance with the regulations.

N. Transition Provisions

1. Effect of Prior Authorizations - Notwithstanding sections (**D**) and (**F**) of this Article (**V**), a Covered Entity may use or disclose PHI, consistent with subsections (2) and (3) below, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of PHI, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.
2. Effect of Prior Authorizations for Other than Research Purposes - Notwithstanding section (**D**) of this Article (**V**), a Covered Entity may use or disclose PHI that it created or received prior to the applicable compliance date of the privacy regulations pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of the privacy regulations, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction.
3. Effect of Prior Permission for Research - Notwithstanding sections (**D**) and (**F**)(9) of this Article (**V**), a Covered Entity may, to the extent allowed by one of the following permissions, use or disclose, for research, PHI that it created or received either before or after the applicable compliance date of the privacy regulations, provided that there is no agreed-to restriction, and the Covered Entity has obtained, prior to the applicable compliance date, either:

   a. An authorization or other express legal permission from an individual to use or disclose PHI for the research;
   b. The informed consent of the individual to participate in the research; or
   c. A waiver by an IRB of informed consent in accordance with federal regulations, provided that a Covered Entity must obtain the authorization in accordance with section (**D**) of this Article if, after the compliance date, informed consent is sought from an individual participating in the research.
4. Effect of Prior Contracts or Arrangements with Business Associates -

Notwithstanding any other part of the privacy regulations, a Covered Entity, other than a small health plan, may disclose PHI to a business associate and may allow a business associate to create, receive or use PHI on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with the requirements of the privacy regulations pertaining to business associates consistent with the requirements, and only for such time, set forth in subsection (5) below.

5. Deemed Compliance
   a. Qualification - Notwithstanding any other part of the privacy regulations, a Covered Entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements pertaining to business associates, with respect to a particular business associate relationship, for the time period set forth in (b) below, if:
      i. Prior to October 15, 2002, such Covered Entity has entered into and is operating pursuant to a written contract or arrangement with a business associate for such business associate to perform functions or 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.
   b. Limited Deemed Compliance Period - A prior contract or other arrangement that meets the qualification requirements in this subsection (5), shall be deemed compliant until the earlier of:
      i. The date such contract or other arrangement is renewed or modified on or after the compliance date; or
      ii. April 14, 2004.
   c. Covered Entity Responsibilities - Nothing in this section shall alter the requirements of a Covered Entity to comply with the compliance and enforcement regulations of HIPAA, and the requirements pertaining to access to PHI, accounting of disclosures of PHI, amendment of PHI and mitigation of harmful effects with respect to PHI held by a business associate.

The Compliance Date for the Privacy Standards is April 14, 2003.

VI. Security Requirements

The Security Requirements apply to Health Plans, and Health Care Clearinghouses or Health Care Providers who either 1) process any electronic transmission between entities or 2) electronically maintain any health information used in an electronic transmission that has been sent or received between health care entities. Hybrid Entity concept does not apply. Entire institution is covered entity if one component is covered. FERPA exception does not apply.

A. Administrative procedures - documented, formal practices to manage the execution and selection of security measures to protect data and to manage the conduct of personnel to protect data, i.e. audits, training, disaster recovery.

B. Physical safeguards - protection of physical computer systems, buildings and equipment from fire, natural and environmental hazards and intrusion. Must appoint a security officer.

B. Technical security services - processes put in place to protect information and control individual access to information such as passwords, encryption, entity authentication.

B. Technical security mechanisms - processes put in place to guard against unauthorized access to data transmitted over a network, such as message authentication, encryption, alarms, event reporting.

B. Standards for electronic signature.

The Security regulations are not yet finalized. When final regulations are issued, they will go into effect two years from the date of issuance.

VII National Identifiers

HIPAA requires the Secretary of DHHS to adopt standards providing for a standard unique identifier for each individual, employer, health plan, and health care provider for use in the health care system.

So far, only the regulations regarding the National Employer Identifiers have been finalized, with an effective date of July 30, 2004. National Identifiers for providers, individuals and payors have not yet been finalized.

VIII Preemption of State Law

In general, HIPAA preempts provisions of state law which are contrary to HIPAA. This general rule does not apply if one of the following conditions is met:

A. The Secretary of DHHS has made a determination that the state law should not be preempted.
B. The state law relates to the privacy of health information and is more stringent than HIPAA.
C. The state law provides for the reporting of disease or injury, child abuse, birth, death, or for public health surveillance, investigation or intervention.
D. The state law requires health plans to report or allow access to information for audit or licensing purposes.

IX Compliance and Enforcement

A person who believes a covered entity is not in compliance with HIPAA may file a complaint with the Secretary of DHHS. The Secretary may investigate complaints and may also conduct compliance reviews to determine compliance. A covered entity must:

D. Provide records and compliance reports as required by the Secretary.
E. Cooperate with complaint investigations and compliance reviews.
F. Permit access to information by the Secretary.

X **Penalties**

A. General

In general, the Secretary shall impose on anyone who violates a provision of HIPAA a penalty of not more than $100 for each such violation, except that the total amount imposed on a person for violations of an identical requirement during a calendar year may not exceed $25,000. There are limitations on this penalty when the failure to comply is due to reasonable cause and is cured within 30 days, when the noncompliance was not known and could not have reasonably been known by the person, and when other penalties apply.

B. Wrongful Disclosure

A person who knowingly and in violation of HIPAA

3. Uses or causes to be used a unique health identifier;
4. Obtains individually identifiable health information relating to an individual; or
5. Discloses individually identifiable health information to another person,

shall be punished as follows:

1. Be fined not more than $50,000 imprisoned not more than one 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 the 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.