Significant Features of Medical Information Privacy Regulations
January 12, 2001

James C. Pyles, Esq.
Powers, Pyles, Sutter and Verville, P.C.
1875 Eye St., N.W.
Washington, D.C. 20006
(202) 466-6550
e-mail: jpyles@ppsv.com

I. Significance

A. Establishes the first "set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care". 65 Fed. Reg. at 82464

B. All 50 states recognize a right to privacy under their tort laws. *Id.*

C. The United States Supreme Court has recognized constitutional protection for health information privacy and has also recognized that therapist-patient communications are "privileged" and cannot be disclosed without patient consent. Whalen v. Roe, 429 U.S. 589 (1977); Jaffee v. Redmond, 116 S.Ct. 1923 (1996)

D. Accordingly, the standards contained in these regulations are likely to be viewed increasingly as the minimum national standards that must be met by those who handle identifiable health information.

II. When effective

A. Published in the Federal Register December 28, 2000 (65 Fed. Reg. 82462)

B. Effective date is February 26, 2001(65 Fed. Reg. 82462)

C. Compliance dates—"no later than"
1. For health care providers—February 26, 2003
2. For health plans—February 26, 2003
3. For "small" health plans (annual receipts of less than $5 million)—February 26, 2004
4. Health care clearinghouses—February 26, 2003 (45 CFR 164.534)

III. Sources of potential liability for violation of privacy right

A. Tort law—generally common law

B. Medical malpractice

C. Invasion of privacy

D. Breach of physician-patient confidential relationship

E. Violation of statute or regulations governing licensing of physicians

F. Breach of fiduciary duty of confidentiality

G. Breach of implied contract to keep personal information private

H. Breach of state statute relating to physician-patient confidentiality

I. Medicare conditions of participation
   1. Hospitals—42 CFR 482.13
   2. Skilled nursing facilities—section 1819(c)(1)(iii) and (iv)
   3. Home health agencies—section 1891(a)(1)(C)

J. Joint Commission on Accreditation of Healthcare Organizations

K. Elements for liability under tort law
   1. Duty
   2. Breach
   3. Damages

L. Only about one-half of states have general laws that prohibit disclosure of health information without authorization. 65 Fed. Reg. at 82473
   1. These regulations preempt state law that is "contrary"—where "State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable." 45 CFR sec. 160.202-203
   2. Regulations also leave in effect state privacy laws that are "more stringent".
   3. State law is defined as including, "a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law."
   4. Does this mean that under these regulations consent would be required in all 50 states? Probably.

IV. Who is covered?

A. A “covered entity” which includes
   1. Health plans
   2. Health care clearinghouses and
   3. Health care providers who transmit any health care information in electronic form in connection with a transaction covered by HIPAA. (45 CFR 160.103)
      a. Health care providers are defined as “providers” under the Medicare program and “anyone who furnishes, bills, or is paid for health care in the normal course of business” (45 CFR 160.103)

B. Business associates (pursuant to a business associates contract) (45 CFR 164.504(e))
   1. “Business associate” is defined as anyone who performs or assists a covered entity in an activity that involves the use or disclosure of individually identifiable health information—includes legal, actuarial, accounting, consulting, data aggregation, management and administration, utilization review, quality assurance, billing, benefit management, practice management and repricing. (45 CFR 160.103)

   2. A covered entity may disclose protected health information to a business associate and allow a business associate to receive such information on its behalf if it has a “written contract” that does the following:
      a. Establishes the permitted and required uses and disclosures for such information and does not authorize the business associate “to use or further disclose” the information in a manner that would violate the regulations if done by a covered entity (there are exceptions for management and administration of the business associate and data aggregation services relating to health care operations of the covered entity).
      b. Provides that the business associate
         1. will not further disclose the information other than as permitted or required by contract or law;
         2. use appropriate safeguards to prevent use or disclosure of the information “other than as provided for by contract”;
         3. report to the covered entity any use or disclosure not permitted by the contract;
         4. ensure that any agents or subcontractors to whom the business associate provides protected health information agree to the same restrictions and conditions;
         5. make available protected health information to which an individual has a right of access under these regulations;

6. Make available protected health information for amendment at the request of an individual as provided under these regulations;
7. Make available information required for an accounting of disclosures required by these regulations;
8. Make available to the Secretary "internal practices, books, and records relating to the use and disclosure of protected health information" for the purposes of determining the covered entity's compliance with these regulations; and
9. At the termination of the contract, return or destroy all protected health information (if feasible) and retain no copies. (45 CFR 164.502(e); 164.504(e))

V. What is covered?

A. "Protected health information" which means "individually identifiable health information" that is
   1. transmitted by electronic media;
   2. maintained in any electronic medium; or
   3. transmitted or maintained in "any other form or medium". (45 CFR 164.501)

B. "Individually identifiable health information" is health information that
   1. Is "created or received" by a covered entity and
   2. relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care or the past, present or future payment for the provision of health care to an individual and
      a. identifies the individual or
      b. there is a "reasonable basis" to believe the information can be used to identify the individual. 45 CFR 164.501
      [Note—information is not individually identifiable if (a) a person with appropriate knowledge and experience with accepted statistical and scientific principles determines that the risk of identification is "very small" or (b) specific identifiers are removed. (45 CFR 164.514(b))**]**
      c. excludes records covered by the Family Educational and Privacy Act. (45 CFR 164.501)

VI. Background

A. The statutory provisions calling for health information privacy standards were contained in sections 261-264 of the "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) enacted August 21, 1996. 65 Fed. Reg. at 82469.

1. Administrative Simplification was part of the Health Security Act debated in the Senate in 1994.
2. The House passed a version that included privacy provisions.
3. The Conference Committee moved privacy to section 264 and deferred action.
4. Section 262 of HIPAA directs the Secretary to issue standards to facilitate electronic exchange of information
5. Section 264(b) required the following
    a. The Secretary of Health and Human Services to submit to Congress recommendations for
        1. rights that an individual who is the subject of individually identifiable health information "should have"
        2. procedures for exercising those rights and
        3. uses and disclosures that should be authorized or required. 65 Fed. Reg. at 82469-70.
    b. If Congress did not enact standards by August 21, 1999, the Secretary was to issue final regulations no later than February 21, 2000.

B. Response to HIPAA
    1. Congress did not enact legislation.
    2. The Secretary issued recommendations on September 11, 1997.
    3. The Secretary issued proposed rules on November 3, 1999 (64 Fed. Reg. 59918).

C. This is the second set of final regulations to implement HIPAA
    1. The "Transaction Rule" was issued on August 17, 2000 (65 Fed. Reg. 50312)
    2. Regulations still to be issued
        a. unique identifiers for employers to use in electronic health care transactions
        b. unique identifiers for providers to use
        c. standards for security of electronic information systems
        d. unique identifiers for health plans
        e. standards for claims attachments
        f. standards for coordination of benefits
        g. enforcement regulations

D. What the regulations do

    1. Establish standards for privacy protections of individually identifiable health information and the processes for implementing those standards and
    2. Establish rights and processes for individuals to obtain access to and correct personal health information

VII. Privacy **protections and processes**

A. The regulations are organized around 3 privacy protections
   1. Consent
   2. Authorization
   3. Agreement or opportunity to object

B. The regulations describe two broad categories of "uses or disclosures"
   1. Those for which consent, authorization or agreement/opportunity to object are required (45 CFR 164.506, 508, and 510) and
   2. Uses and disclosures for which none of the above are required (45 CFR 164.512).

VIII. Uses and disclosures for which **consent** is required (45 CFR 164.506)

A. A "covered health care provider" in a direct treatment relationship with an individual must obtain the individual's consent prior to using or disclosing protected health information to carry out "treatment, payment or health care operations". The provider need not obtain consent for treatment, payment or health care operations purposes if the provider is in an "indirect treatment relationship" with the individual (45 CFR 164.506(a)(1) and (2))

B. Exceptions
   1. Emergency treatment, if the provider attempts to obtain consent "as soon as reasonably practicable" after the delivery of treatment;
   2. Treatment as required by law and the provider has attempted to obtain consent; or
   3. The provider tries, but is unable to obtain consent due to substantial barriers to communication and the provider "determines, in the exercise of professional judgment" that consent is "clearly inferred" from the circumstances. 45 CFR 164.506(a)(3)

C. Conditioning treatment or enrollment on consent
   1. A provider may condition "treatment" on the provision of consent. 45 CFR 164.506(b)(1)
   2. A health plan may condition "enrollment" on the provision of consent
   3. Consent may not be combined in a single document with notice of rights. 45 CFR 164.506(b)(3)

D. Consent must
   1. Inform the individual that protected health information may be used and disclosed to carry out treatment, payment or health care operations;

2. State that the individual has a right to review the notice of rights before signing the consent;
3. Inform the individual of the right "to request" a restriction on how the information will be used or disclosed for treatment, payment, or health care operations;
4. Inform the individual that the entity is not required to agree to the request for a restriction;
5. Inform the individual of the right to revoke the consent in writing; and
6. Be signed and dated.

E. Treatment, payment and health care operations are defined as follows:
   1. Treatment—the provision, coordination, or management of health care and related services by "one or more health care providers", consultations between providers relating to a patient, and the referral of a patient from one provider to another (45 CFR 164.501).
   2. Payment—activities by a health plan to obtain premiums or to make coverage determinations and payment (including billing, claims management, reviews for medical necessity and appropriateness of care and utilization review and preauthorizations or by a covered health care provider to obtain or provide reimbursement).
   3. Health care operations—any of the following activities by a covered entity:
      a. quality assessment and improvement activities;
      b. reviewing competence or qualifications of health care professionals;
      c. underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts;
      d. conducting or arranging for medical review, legal services, and auditing functions including fraud and abuse compliance programs;
      e. business planning and development;
      f. business management and general administrative activities of the entity (including "creating de-identified health information").

IX. Uses and disclosures for which **authorization** is required (45 CFR 164.508)

A. A "covered entity" may not use or disclose protected health information without an authorization that is valid. 45 CFR 164.508
   [Note—The preamble states that 164.508(a) does not require authorization for treatment, payment or health care operations. 65 Fed. Reg. at 82513. While this was true of the proposed rule, the language of the final version of 508(a) does not contain that limitation.**]**

B. Authorization is required for use or disclosure of **"psychotherapy notes"** except
   1. In case of treatment, payment or health care operations (assuming consent has been granted)
      a. where the information is to be used by the originator of the psychotherapy notes for treatment;
      b. the information is to be used or disclosed by the covered entity in "training programs" in mental health or
      c. the information is used or disclosed by the covered entity to defend a legal action or other proceeding brought by the individual
   2. Other situations in which psychotherapy notes can be disclosed without authorization
      a. To obtain compliance with these regulations
      b. When disclosure is otherwise required by law
      c. When the information is to be disclosed to a health oversight agency for health oversight of the originator
      d. When the information is to be disclosed to a coroner, medical examiner or funeral director as necessary to carry out their duties or
      e. Where disclosure is necessary "to prevent or lessen a serious and imminent threat to the health or safety" of a person or the public (if disclosure is consistent with "applicable law and standards of ethical conduct").
         [Note: It would also appear that an authorization for psychotherapy notes could be altered or waived for research purposes by an IRB or by a privacy board. See 164.512(i). Consent would still be required.**]**
   3. "Psychotherapy notes" is defined to mean notes recorded "in any medium" by a health care provider who is a "mental health professional" documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are "separated from the rest of the individual's medical record".
      a. The term excludes
         1. medication prescription and monitoring;
         2. counseling session start and stop times;
         3. the modalities and frequencies of treatment furnished;
         4. results of clinical tests; and
         5. any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. (45 CFR 164.501)

C. Conditioning treatment or payment on provision of authorization

1. A covered entity may not condition treatment, payment, enrollment in a health plan or eligibility for benefits on the provision of authorization except in the following circumstances:
   a. A covered health care provider may condition research-related treatment;
   b. A health plan may condition enrollment in the plan or eligibility determinations relating to the individual or for underwriting or risk rating determinations; and
   c. A health plan may condition payment of a claim where disclosure is necessary to determine payment for the claim and the plan seeks disclosure of information to it by another covered entity. 45 CFR 164.508(b)(4) (iii) (e) (1).
2. A health plan may not condition enrollment, eligibility or payment of a claim on the authorization of use or disclosure of psychotherapy notes. 45 CFR 164.508(b)(4)(ii)(B) and (iii)(B)

D. Core elements to be included for authorization to be valid
   1. A description of the information to be used or disclosed
   2. The name or other specific identification of the "person(s), or class of persons" authorized to make the requested use or disclosure
   3. The same information for the persons to whom the use or disclosure will be made
   4. An expiration date
   5. A statement of the individual's right to revoke in writing and the process to be followed
   6. A statement that the information may be subject to redisclosure and no longer protected by the regulations
   7. Signed and dated

E. Authorizations requested by a covered entity for its own use or disclosure must contain the following additional elements
   1. A statement that the covered entity will not condition treatment, payment, enrollment in a health plan or eligibility for benefits on authorization
   2. A description of each purpose of the requested use or disclosure
   3. A statement that the individual may inspect or copy protected health information as permitted under the regulations and refuse to sign the authorization
   4. A statement disclosing whether the covered entity will receive direct or indirect remuneration from a third party as a result of the use or disclosure. 45 CFR 164.508(d).

X. Uses and disclosures requiring an **opportunity for individual to agree or object** (45 CFR 164.510)

A. Facility directories

1. Covered health care providers may use the following protected information to main a directory in its facility “except when an objection is expressed”
    a. The individual’s name, location in the facility, condition in general terms (that does not communicate specific medical information), and religious affiliation. (45 CFR 164.510(a))
2. Covered health care providers may “disclose” for directory purposes the above information
    a. To members of the clergy or
    b. To other persons who ask for the individual by name (except for religious affiliation)
3. Covered health care providers must inform individuals of the protected health information that may be included in a directory and the persons to whom it may disclose that information and provide the individual with the opportunity “to restrict or prohibit some or all of the uses or disclosures”.
4. In emergency situations where the opportunity to object cannot be provided, the provider may use or disclose some or all of the protected information listed above in accordance with the individual’s “best interest” or the provider’s judgment of the individual’s best interest.

B. Involvement in the individual’s care
1. Covered entities may disclose protected health information that is “directly relevant” to such person’s involvement in the care if the entity obtains individual’s consent or provides the individual with an opportunity to object and no objection is expressed. (45 CFR 164.510(b))
2. If an opportunity to object cannot be “practicably” provided, the entity is to use its professional judgment to determine whether a disclosure is in the best interest of the individual.
3. These requirements are to apply in cases of disaster relief only to the extent that, in the exercise of professional judgment, the requirements do not interfere with the ability to respond to emergency circumstances.

XI. Uses and disclosures for which **consent, authorization, or opportunity to object is not required** (45 CFR 164.512)

A. As required by law (45 CFR 164.512(a))
1. Covered entities may use or disclose protected health information “to the extent” that such use or disclosure is required by law.

B. Public health activities (45 CFR 164.512(b))
1. Covered entities may disclose protected health information for public health activities to

a. A public health authority authorized by law to collect or receive such information;
b. A person under the jurisdiction of the Food and Drug Administration to report product defects, to track products, to permit product recalls and to conduct post marketing surveillance;
c. A person who may have been exposed to a communicable disease or be at risk of spreading a disease or condition, if authorized by law; and
d. A health care provider who is a member of an employer's workforce about a member of the workforce who has requested and receives health care from the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a workplace related injury.

C. Disclosures about abuse, neglect, domestic violence (45 CFR 164.512(c))
   1. A covered entity may disclose protected health information about an individual that it "reasonably believes" to be a victim of abuse, neglect, or domestic violence to authorities authorized by law to receive such information.
   2. The covered entity must "promptly inform" the individual that such a disclosure has been or will be made unless that notice would cause a risk of serious harm.

D. Health oversight activities (45 CFR 164.512(d))
   1. A covered entity may disclose protected health information to a "health oversight agency" for "oversight activities authorized by law".
   2. A "health oversight activity" does not include an investigation or other activity "that does not arise out of and is not directly related to"
      a. the receipt of health care,
      b. a claim to public benefits related to health or
      c. qualification for, or receipt of public benefits or services when the patient's health is integral to the claim.

E. Judicial and administrative proceedings (45 CFR 164.512(e))
   1. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding
      a. to the extent expressly authorized by an order from the court or tribunal, or
      b. in response to a subpoena, discovery request or other lawful process if the covered entity receives "satisfactory assurances" from the party seeking the information that the individual who is the subject of the information has been given notice of the

request, or that “reasonable efforts” have been made to secure a “qualified protective order”.

2. A covered entity will be deemed to have received “satisfactory assurances” if it receives a written statement and accompanying documentation that
    a. the requesting party has made a “good faith attempt” to provide written notice to the subject of the information,
    b. the notice provided sufficient information about the proceeding to permit the individual to raise an objection, and
    c. no objections were raised or they were resolved in favor of disclosure by the court or tribunal.
3. A “qualified protective order” is an order from a court or administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding and requires the return or destruction of the information (including all copies) at the end of the litigation or proceeding.

F. Law enforcement purposes (45 CFR 164.512(f))
    1. A covered entity may disclose protected health information “for law enforcement purposes” if the following processes, as applicable, are met
        a. the disclosure is required by law;
        b. the disclosure is to comply with the requirements of a court order, or court-ordered warrant, a subpoena issued by a judicial officer, a grand jury subpoena, or
        c. an administrative request, including an administrative subpoena or summons, a civil or authorized investigative demand or similar process authorized by law.
        d. When the request is in the form of an “administrative request”, there must be a showing that
            1. the information sought is relevant and material to a legitimate law enforcement inquiry;
            2. the request is “specific and limited in scope…in light of the purpose for which the information is sought”; and
            3. “de-identified” information could not be used.
    2. A covered entity may disclose protected health information in response to a law enforcement official’s request for the purpose of “identifying, or locating a suspect, fugitive, material witness, or missing person”.
        a. The information that may be disclosed is limited to name and address, date and place or birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical features.

b. The covered entity may not disclose for this purpose “any protected health information related to the individual’s DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue”.

3. A covered entity may disclose protected health information in response to a law enforcement official’s request for such information “about an individual who is or is suspected to be a victim of a crime” but only if
   a. the individual agrees to the disclosure; or
   b. the covered entity is unable to obtain the individual’s agreement because of emergency circumstances and the law enforcement official “represents” (can be verbally) that the information is not intended to be used against the individual, that the immediate law enforcement activity would be “materially and adversely affected” by waiting to obtain the individual’s agreement and disclosure “is in the best interest of the individual” as determined by the exercise of the covered entity’s best judgment.
4. A covered entity may disclose protected health information to a law enforcement official about a deceased individual for the purpose of alerting the official that the entity “has a suspicion that such death may have resulted from criminal conduct”.
5. A covered entity may disclose to a law enforcement official protected health information that the covered entity “believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity”.
6. A covered health care provider providing emergency health care other than on the provider’s premises may disclose protected health information to a law enforcement official if such disclosure “appears necessary” to alert law enforcement to the commission of a crime, the location of crime victims, and the identity of the perpetrator of the crime.

G. Disclosures about decedents to coroners, medical examiners and funeral directors (45 CFR 164.512(g))
   1. A covered entity may disclose protected health information to coroners and medical examiners for the purpose of identifying a deceased purpose determining the cause of death or for other duties as authorized by law.
   2. An entity may disclose protected health information to funeral directors “consistent with applicable law” as necessary to carry out their duties with respect to the decedent.

H. Uses and disclosures for cadaveric organ, eye or tissue donation purposes (45 CFR 164.512(h))
   1. A covered entity may use or disclose protected health information

to organ procurement organizations or other organizations and other organizations involved in organ transplantation “for the purpose of facilitating organ, eye, or tissue donation or transplantation”.

I. Uses and disclosures for research purposes (45 CFR 164.512(h))
   1. A covered entity may use or disclose protected health information “for research, regardless of the source of funding” provided that it obtains documentation of “an alteration to or waiver, in whole or in part, of the individual authorization” required by the regulations that has been approved by either
      a. an Institutional Review Board (IRB) that meets federal regulatory requirements or
      b. a “privacy board” that
         1. has members with “varying backgrounds and appropriate professional competency as necessary” to review the effect of the research protocol on the individual’s privacy rights and related interests;
         2. includes at least one member who is not “affiliated” with the covered entity or any entity conducting or sponsoring the research and
         3. does not have any member participating in a review of any project “in which the member has a conflict of interest”.
   2. The documentation necessary for approval of an alteration or waiver must include the following findings
      a. the use or disclosure of protected health information involves no more than “minimal risk to the individuals”;
      b. the alteration or waiver of authorization “will not adversely affect the privacy rights or the welfare of the individuals”;
      c. the research “could not practicably be conducted without the alteration or waiver”;
      d. the research “could not practicably be conducted without access to and use of the protected health information”;
      e. the “privacy risks” to the individuals whose protected health care information is to be used “are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research”;
      f. there is an “adequate” plan to protect the identifiers from improper use and disclosure;
      g. there is an adequate plan to destroy the identifiers “at the earliest opportunity” consistent with the conduct of the research, unless there is a health or research justification for retaining them;
      h. there are “adequate written assurances” that the protected health information will not be reused or disclosed to any other

person or entity except as authorized by law, for authorized oversight of the research project, or for other research projects where the use or disclosure would be permitted by these regulations; and

i. the signature of the chair, or other member designated by the chair, of the IRB or privacy board

J. Uses and disclosures to avert a serious threat to health and safety (45 CFR 164.512(j))
   1. A covered entity may disclose protected health information, "consistent with applicable law and standards of ethical conduct" if the entity "in good faith, believes" the use or disclosure
      a. is necessary to "prevent or lessen a serious and imminent threat to the health or safety or a person or the public" and
      b. the disclosure is to a person "reasonably able to prevent or lessen the threat, including the target of the threat".
   2. A covered entity may also disclose protected health information where it is necessary for law enforcement authorities to identify or apprehend an individual because of a statement "admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim" or it appears that the individual has escaped from lawful custody.
      a. The information that may be disclosed is limited to the statement made by the individual and the information that may be disclosed to identify or locate a suspect or fugitive (164.512(f)(2)(I)).
   3. A covered entity may <u>not</u> use or disclose a statement by an individual admitting participation in a violent crime if the entity learns of the information
      a. in the course of treatment "to affect the propensity to commit the criminal conduct" or "counseling or therapy" or
      b. through a request by the individual "to initiate or be referred for treatment, counseling, or therapy".

K. Uses and disclosures for specialized government functions (45 CFR 164.512(k))
   1. A covered entity may use or disclose protected health information with respect to
      a. military and veterans' activities if there has been a notice published in the Federal Register
      b. information needed by the Department of Veterans' Affairs to make a determination about an individual's eligibility for veterans' benefits and
      c. other authorized purposes related to foreign military personnel and national security and intelligence activities.

L. Use and disclosures for workers' compensation (45 CFR 164.512(l))
   1. A covered entity may disclose protected health information "as authorized by and to the extent necessary" to comply with workers' compensation or other similar programs established by law.

XII. **Other requirements and rights** with respect to uses and disclosures of protected health information (45 CFR 164.514)

A. Health information is not individually identifiable health information (and therefore, not protected health information under these regulations) if
   1. a person with "appropriate knowledge of and experience" with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable
      a. applies such principles and methods and determines that the risk is "very small" that information could be used by an anticipated recipient to identify the individual who is the subject of the information and
      b. that expert documents "the methods and the results of the analysis" that justify such determination. (45 CFR 164.514(a))
   2. Alternatively, health information will be deemed not individually identifiable if a specified list of 18 identifiers (such as names, geographic subdivisions smaller than a state, Social Security numbers, and account numbers) for individuals or relatives, employers or household members of the individual are removed.
   3. 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
      a. the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual and
      b. the code or other means of record identification is not disclosed for any other purpose.

B. A covered entity must "reasonably ensure" by applying the following measures that the "minimum necessary" amount of protected health information is used or disclosed (45 CFR 164.514(d))
   1. With respect to uses, a covered entity must identify those persons or classes of persons in its workforce who need access to protected health information to carry out their duties and
   2. Identify the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

3. The covered entity must make “reasonable efforts” to limit the access of such persons to the protected health information for which access is needed to carry out their duties.
4. With respect to disclosures, a covered entity must
    a. For “routine and recurring disclosures”—implement “policies and procedures” that limit the protected health information to the amount “reasonably necessary” to achieve the purpose of the disclosure.
    b. For all other disclosures—develop criteria designed to limit the disclosure of protected health information to the information “reasonably necessary to accomplish the purpose for which the disclosure is sought” and review requests for disclosure “on an individual basis” in accordance with those criteria.

    c. The same type of policies and procedures must be implemented for “requests” by covered entities for protected health information.
5. A covered entity may assume that a requested disclosure is for the minimum necessary information (if such reliance is “reasonable under the circumstances”), when
    a. In making disclosures to public officials, the official represents that the information necessary is the minimum amount necessary;
    b. The information is requested by another covered entity;
    c. The information is requested by a “professional” who is a member of the entity’s workforce or is 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 for the stated purpose; or
    d. Documentation or representations are provided to the covered entity indicating compliance with the requirements for the use or disclosure of protected health information for research purposes.
6. A covered entity may not use, disclose or request “an entire medical record”, in cases where the “minimum necessary” limitation applies, except where the entire record is “specifically justified” as the amount of information reasonably necessary to accomplish the purpose of the use, disclosure or request.
7. The “minimum necessary” limitation does not apply to
    a. disclosures to or requests by “a health care provider for treatment”;
    b. uses or disclosures made to the individual for access to the individual’s medical record or for accounting for disclosures, or disclosures made pursuant to an authorization except for authorizations obtained by a covered entity for its own use, by a covered entity for another covered entity to disclose information for treatment, payment or health care operations, and by a

covered entity for research that involves treatment of the individual. (45 CFR 164.502(b))

C. A covered entity may not use or disclose protected health information for “marketing” without an authorization except that no authorization is required when the information is used to make a marketing communication that
   1. occurs in a “face-to-face encounter” with the individual;
   2. concerns products or services of nominal value;
   3. concerns health-related products and services of the covered entity or a third party and the communication meets the following requirements
      a. The communication identifies the covered entity as making the communication, states whether the covered entity has or will receive direct or indirect remuneration for making the communication, and contains instructions describing how an individual may “opt out” of receiving future marketing communications (unless the communication is contained in a newsletter or similar type of general communication).
      b. If the covered entity uses or discloses protected health information to target individuals based on their health status or condition
         1. the entity must make a determination prior to making the communication that the product or service “may be beneficial to the health of the type or class of individual targeted” and
         2. the communication must explain why the individual has been targeted and how the product or service relates to the health of the individual.
      c. The covered entity must make “reasonable efforts” to ensure that individuals who “opt out” of receiving future marketing communications are not sent those communications.

D. A covered entity may use or disclose the following protected health information without authorization if it is to a business associate or to an institutionally related foundation, for the purposes of “raising funds for its own benefit”
   1. demographic information relating to an individual; and
   2. dates of health care provided to an individual.
   3. A covered entity may not use protected health information for this purpose without an authorization unless the use is mentioned in the notice of privacy practices which must be given to each individual and the fundraising materials sent to an individual include a description of how to “opt out” of receiving further fundraising communications.

E. Prior to any disclosure permitted under the regulations, a covered entity must
   1. "verify the identity" and the "authority" of any such person to have access to protected health information and
   2. obtain any documentation which is required by the regulations for disclosure (45 CFR 164.514(h))

XIII. **Notice** of privacy practices (45 CFR 164.520)

A. An individual "has a right to adequate notice" of
   1. the uses and disclosures of protected health information that may be made by the covered entity, and
   2. the individual's rights and the covered entity's legal duties with respect to protected health information. (45 CFR 164.520(a))

B. The covered entity must provide a notice that contains the following elements:
   1. A header prescribed in the regulation.
   2. A description and at least one example of the types of uses and disclosures the covered entity is permitted to make for each of the following: treatment, payment and health care operations.
   3. A description of each of the other purposes for which the entity is permitted or required to use or disclose protected health information without written consent or authorization.
   4. If a use or disclosure is one that is "prohibited or materially limited" by a "more stringent" state law, the description must reflect that law.
   5. The description in the notice must include "sufficient detail" to place the individual on notice of the uses and disclosures that are permitted or required by these regulations and other applicable law.
   6. A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke the authorization.
   7. A statement of the individual's rights, including
      a. the right to request restrictions on certain uses and disclosures (including a statement that the covered entity is not required to agree to the restriction);
      b. the right to receive confidential communications of protected health information;
      c. the right to inspect and copy protected health information;
      d. the right to amend protected health information;
      e. the right to receive an accounting of disclosures of protected health information; and
      f. the right to receive a paper copy of the notice upon request.
   8. A statement of the covered entity's duties including

a. that the covered entity is “required by law to maintain the privacy of protected health information” and to provide individuals with notice of its legal duties and privacy practices;
b. a statement that the covered entity is required to abide by the terms of the current notice; and
c. a statement that it reserves the right to change a privacy practice and have that change apply to all health information it maintains.

9. The notice must contain a statement informing the individual of the right to file a complaint with the Secretary and that there will be no retaliation.

C. When the notice must be provided
1. A covered health care provider that has a direct treatment relationship with an individual must
a. provide the notice no later than the date of the first service delivery (including services electronically);
b. if the provider maintains a physical delivery site
1. have the notice “available” on request for individuals to take with them and
2. post the notice in a “clear and prominent location”.
2. A covered entity that maintains a web site that provides information about customer services or benefits must prominently post the notice and make it available electronically.
3. A covered entity must make the notice available upon request “to any person”.
4. The regulations contain specific time frames during which health plans must provide the notice.
5. Covered entities participate in organized health care arrangements may provide “joint notice” that meets prescribed requirements in the regulations.

XIV. **Right to request privacy protection** for protected health information (45 CFR 164.522(a))

A. A covered entity must permit an individual “to request” that the entity restrict
1. uses or disclosures of protected health information to carry out treatment, payment or health care operations or
2. disclosures to a relative or family member.

B. A covered entity is not required to agree to a restriction, but if it does, it must comply with that request except where information is needed to treat a patient in an emergency situation.

C. A covered entity must permit an individual to request and "must accommodate reasonable requests" by individuals to receive communications of protected health information by "alternative means or at alternative locations".

XV. **Right to an accounting** of disclosures (45 CFR 164.528)

A. An individual has a "right to receive an accounting of disclosures of protected health information" by the covered entity in the 6 years prior to the date of the request except for disclosures
   1. to carry out treatment, payment and health care operations;
   2. to individuals of protected health information about them;
   3. for a facility's directory or for similar purposes;
   4. for national security or intelligence purposes;
   5. to correctional institutions or law enforcement officials as provided under the regulations; or
   6. that occurred prior to the compliance date for the covered entity.

B. A covered entity must "act on" the individual's request for an accounting "no later than 60 days after receipt of such a request". One 30 day extension of time is permitted.
   1. One accounting in any 12 month period must be provided free of charge.

XVI. **Administrative requirements** (45 CFR 164.530)

A. A covered entity must designate a "privacy official" who is responsible for the development and implementation of policies and procedures implementing these regulations

B. A covered entity must designate a "contact person or office" who is responsible for receiving complaints and who is able to provide further information about matters covered by the notice.

C. A covered entity must train all members of its workforce on the policies and procedures required by the regulations that are necessary for them to carry out their functions by "no later than the compliance date for the covered entity".
   1. Employees must be trained with respect to any changes in policies "within a reasonable period of time" after the change.
   2. Each new member of the work force must be trained "within a reasonable period of time" after joining the workforce.

D. A covered entity must have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information".

E. A covered entity must provide a process for individuals to make complaints about the entity's privacy policies and procedures, its compliance with those policies and procedures, or its compliance with the regulations.
    1. A covered entity must document all complaints and their resolution.

F. A covered entity must have and apply "appropriate sanctions" against members of its workforce who fail to comply with the entity's privacy policies and procedures or the requirements of the regulations.
    1. A covered entity must document all sanctions.

G. A covered entity must "mitigate, to the extent practicable" any harmful effect that is "known" to have resulted from a use or disclosure in violation of these regulations.

H. A covered entity may not "intimidate, threaten, coerce, discriminate against, or take other retaliatory action" against
    1. an individual for the exercise of any right, or the participation in any process, under these regulations or
    2. testifying, assisting or participating in an investigation, compliance review, proceeding, or hearing under these regulations.

I. A covered entity must implement policies and procedures with respect to protected health information that are "reasonably designed, taking into account the size of and the type of activities" undertaken by the entity to ensure compliance.

J. A covered entity must document the policies and procedures required by the regulations in "written or electronic form".
    1. The entity must also document any "action, activity, or designation, required by these regulations
    2. The covered entity must retain this documentation for a period of 6 years from the "date of its creation or the date when it was last in effect, whichever is later".

XVII. **Transition provisions** (45 CFR 164.532)

A. A covered entity may continue to use or disclose protected health information pursuant to a consent, authorization or other express legal permission if it was obtained before the applicable compliance date.

B. A covered entity may use protected health information it "created or received before the applicable compliance date" of the regulations if the information is not "expressly excluded" from a permission and complies with all limitations in that permission.

XVIII. **Access** to protected health information (45 CFR 164.524)

A. An individual has a “right of access to inspect and obtain a copy” of the protected health information about the individual in a designated record set “for as long as the information is maintained in the record set” except for
   1. psychotherapy notes;
   2. information compiled in “reasonable anticipation of a criminal or civil judicial or administrative proceeding;” or
   3. protected health information that is subject to, or specifically exempt from the Clinical Laboratory Amendments of 1988.

B. A covered entity may deny access to protected health information provided that the individual is given a “right” to have such denials reviewed.

C. The permitted grounds for denial are
   1. where a licensed health care professional has determined that access requested is “reasonably likely to endanger the life or physical safety” of the individual or another person;
   2. the protected health information makes reference to another person and the licensed health care professional has determined that access is “reasonably likely to cause substantial harm to such other person”.

D. The review is to be performed by a licensed health care professional designated by the covered entity who did not participate the decision to deny access.
   1. The covered entity must comply with the review decision.

E. A covered entity must “act on” a request for access “no later than 30 days after receipt of the request”.

F. An individual also has “the right to have a covered entity amend protected health information or a record about the individual” in a designated record set.
   1. A covered entity must “act on” a request to amend protected health information “no later than 60 days after receipt of such request”.

XIX. **Preemption of state law**

A. Standards, requirements and implementation specifications under the regulations preempt contrary provisions of State law with the following exceptions

1. Where the Secretary makes a determination that a provision of state law
    a. is necessary
        1. to prevent fraud and abuse related to the provision of health care;
        2. to ensure appropriate State regulation of insurance and health plans;
        3. for State reporting on health care delivery or costs; or
        4. for the purposes of serving a "compelling need related to public health, safety, or welfare" if the Secretary determines that the intrusion into privacy is warranted "when balanced against the need to be served"; or
    b. has as its principal purpose the regulation of the manufacture, registration, distribution dispensing or other control of any controlled substance.
2. The provision of State law "relates to the privacy of health information" and is "more stringent" than the requirements of the regulations.
3. State law means "a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law".

XX. **Enforcement**

A. The Secretary will "to the extent practicable" seek cooperation of covered entities in obtaining compliance with the regulations (45 CFR 160.304)
    1. The Secretary will supply technical assistance to covered entities to help them voluntarily comply.

B. Any person who believes that a covered entity is not complying with the regulations may file a complaint with the Secretary.

C. The Secretary may investigate complaints and conduct "compliance reviews" to determine whether covered entities are complying with the requirements of the regulations.

D. A covered entity must permit access to the Secretary during normal business hours and keep such records and provide such compliance reports as the Secretary determines necessary to ensure compliance with the regulations.

E. The Secretary will attempt to resolve complaints "by informal means whenever possible". If the matter cannot be resolved informally, the Secretary will provide the covered entity with findings documenting non-compliance.

F. Penalties (section 1176 of the Social Security Act)
   1. $100 for each violation up to a total of $25,000 for violations of “an identical requirement or prohibition during a single calendar year”.
      a. penalty cannot be imposed if the failure to comply was due to “reasonable cause and not willful neglect” and was corrected within 30 days of the time a person using “reasonable diligence” would have known about it.
      b. The period for correction may be extended by the Secretary based on the “nature and extent of the failure to comply”.
      c. The Secretary may waive a penalty “to the extent that the payment of such penalty would be excessive relative to the compliance failure involved”.
   2. A person who “knowingly” violates the regulations shall be punished by
      a. a fine of up to $50,000 and/or imprisonment of up to one year;
      b. if the violation is committed under “false pretenses”, a fine of up to $100,000 and/or imprisonment for up to five years; and
      c. if the offense is committed “with the intent to sell, transfer or use individually identifiable information for commercial advantage, personal gain or malicious harm”, a fine of up to $250,000 and/or imprisonment for up to ten years.