Hickman & Lowder Co. L.P.A.

Franklin J. Hickman
Janet L. Lowder
David A. Myers
Elena A. Lidrbauch
Sandra J. Buzney
Judith C. Saltzman
Mary B. McKee
Amanda M. Buzo
Lisa M. Garvin

Penton Building
1300 East Ninth Street
Suite 1020
Cleveland, OH 44114
Telephone (216) 861-0360
Fax (216) 861-3113

5062 Waterford Dr.
Sheffield Village, OH 44035
Telephone (440) 323-1111
Fax (440)323-4284

ANALYSIS OF THE HIPAA PRIVACY RULES FOR DD BOARDS

Elena A. Lidrbauch
Franklin J. Hickman
December 2009

Table of Contents

I. Information Covered by the HIPAA Privacy Rules

The HIPAA Privacy Rules cover health plans, health care clearinghouses, and health care providers with respect to Protected Health Information to the extent that any health information is transmitted in electronic form. 45 C.F.R. § 164.104[1].

Protected Health Information means individually identified health information transmitted or maintained in any form, whether electronic, written or oral. § 164.501. Certain education records, including records of therapy involving students over 18 are not subject to the HIPAA privacy regulations. Id.

Electronic transmissions can include transmissions through the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, compact disk media or flash drives. § 162.103.

II. DD Boards are Subject to HIPAA Requirements

DD Boards will generally be covered under HIPAA requirements as both Health Plans and Health Care Providers to the extent that any health information is transmitted in electronic form. DD Boards may also function as Health Care Clearinghouses and Business Associates. COGs made up of DD Boards may be Organized Health Care Arrangements. These concepts are described in detail in the summary which follows.

A. DD Boards as Health Care Providers

DD Boards are covered as Health Care Providers. *Health care provider* means, in summary, a provider of health care services or an organization which furnishes, bills, or is paid for health care in the normal course of business. § 160.103.

Health care under HIPAA is defined as care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, 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. § 160.103.

B. DD Boards as Health Plans

DD Boards are covered as Health Plans to the extent that boards pay for the costs of health care, including Medicaid services.[2]

---

[1]All references are to 45 CFR unless otherwise noted.

[2] *Health plan* means an individual or group plan that provides, ***or pays*** the cost of, medical care. *Health plan* includes the following, singly or in combination:

C. DD Boards as Health Care Clearinghouses

An DD Board may be a Health Care Clearinghouse to the extent that the board processes payment data into a different format.[3] § 160.103. While DD Boards are not doing so currently, if a DD Board agreed to assist a Provider in formatting data or payment submissions to conform to HIPAA requirements, an DD Board would thereby function as a clearinghouse.

The commentary notes that "an entity is considered a health care clearinghouse only to the extent that it meets the criteria in this definition" and "perform[s] the functions in the definition." 65 Fed. Reg. 82477[4].

---

1. The Medicaid program under title XIX of the Act, 42 U.S.C. § 1396, et seq.

2. Any other individual or group plan, or combination of individual or group plans, that provides ***or pays*** for the cost of medical care.

§160.103 (emphasis added)

[3] Under the statute, the term "health care clearinghouse" means "a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements." 42 U.S.C. § 1320d(2). The regulations expand the definition to cover an entity that does either of the following:

(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.

§160.103.

[4]References to the Volume 65 of the Federal Register are to 65 Fed. Reg. No. 250, Part II, December 28, 2000 pp. 82461-82829.

D. Other Roles of DD Boards under HIPAA

DD Boards may function in other capacities, including business associate (see section XIV), or hybrid entity (see section XVI.A). COGs made of DD Boards may function as Organized Health Care Arrangements[5] or as other types of configurations summarized in section XVI.

Are COGS Organized Health Care Arrangements?

A COG would be an OHCA only for those functions which it performs for all members of the COG and the members hold themselves out as acting jointly. To the extent that the COG is doing specific tasks for each board according to the contract, the COG is acting as a Business Associate.

---

[5]The definition of *Organized health care arrangement* includes the following:

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

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

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

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

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

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. § 164.501.

III. General Rules

A. Use and Disclosure

Covered entities, including Health Plans and Health Care Clearinghouses, are permitted to use or disclose protected health information as follows:

1. To the individual;
2. For treatment, payment or health care operations; under HIPAA rules a covered entity may, but is not required, to obtain consent for treatment, payment or health care operations. Ohio law permits only disclosure of the identity of an eligible individual for purposes of treatment and payment. Transfer of information requires a release from individual.
3. Incidental uses and disclosures that occur as a by-product of a use or disclosure otherwise permitted under the Privacy Rule[6], provided that:
   (a) there are adequate safeguards and
   (b) disclosure meets the minimum necessary standard summarized in III.C.
4. Pursuant to and in compliance with a proper authorization;
5. As part of Limited Data Sets which meet requirements summarized in section VIII.C and which are covered by a Data Use Agreement;
6. Pursuant to an agreement authorized by the regulations; under, or as otherwise permitted by, § 164.510; and
7. When the regulations do not require authorization.

§ 164.502(a)(1).

OHIO LAW PRE-EMPTION

RC 5126.044 requires individual's consent for treatment and release from individual to disclose any PHI (other than the individual's identity if necessary for treatment or payment) to entity other than DD Board or Provider in preparation of any ISP. RC 5126.044(B). In general, a release is required for contacts outside covered entity.

[6]The example given in the commentary to the amended rules is that a provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room. Assuming that the provider made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental disclosure resulting from such conversation is permissible under the Rule.

B. Required Disclosures

Records must be disclosed to individuals upon request, subject to certain limitations, and to HHS during compliance reviews. § 164.502(a)(2).

C. Scope of Disclosures

In general, use, disclosure or requests of records must be limited to the minimum which is reasonably necessary to accomplish the purpose of the use, disclosure or request. § 164.502(b)(1).

The ARRA states that, effective February 17, 2010, a covered entity complies with the minimum necessary requirement if the covered entity releases a limited data set or the minimum information necessary to accomplish the purpose of the disclosure. ARRA § 13405(b)(1)(A). The Secretary of HHS is required to issue guidance on what constitutes minimum necessary by August, 2010. ARRA § 13405(b)(1)(B). Once the guidance is issued, the guidance will be definitive.

The covered entity must establish policies which address scope of permissible use by employees, disclosures and requests for information by the entity to ensure that the minimum necessary standard is met. § 164.514(d). The Secretary of HHS will be issuing guidelines by August, 2010 which give further guidance on minimum necessary standards. § ARRA 13405(b)(1)(a).

The minimum necessary requirement does not apply to:

1. Disclosure for treatment purposes;
2. Requests by individuals, with exceptions;
3. Disclosure pursuant to an authorization; and
4. Certain investigations and legal procedures.

§ 164.502(b)(2).

D. Agreed-upon Restrictions

A covered entity may voluntarily agree to restrict disclosure of information. If there is such an agreement, the entity must abide by the terms of the agreement. § 164.502(c).

E. Deceased Individuals

A covered entity must comply with the requirements of HIPAA rules with respect to the protected health information of a deceased individual. § 164.502(f). The covered entity may disclose information on the deceased individual to a person who has authority to act on behalf of a

deceased individual or of the individual's estate, such as an executor or administrator. § 164.502(g)(4).

F. Personal Representatives

In general, a personal representative is treated as the individual for purposes of HIPAA Privacy Rules. § 164.502(g)(1). A personal representative is a person or entity which has legal authority to act on behalf of another. § 164.502(g).

A covered entity may refuse to give information to a personal representative in abuse situations if the covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative. § 164.502(g)(5).

OHIO LAW PRE-EMPTION

Ohio law requires a personal representative to be a legally authorized person or entity, such as a guardian, parent of a minor, legally appointed custodian or person holding a valid power of attorney. Otherwise the person acting as a representative must have a release from the individual.

G. Minors

The Privacy Rules adopt state law governing the right of parents[7] to release or access records of minors. If the parent is not the personal representative of the minor (e.g. custody was removed by Juvenile Court) and state law is not clear on access by such parent, the Privacy Rules create a right for a professional to exercise professional judgement on whether to allow access by such parent. § 164.502(g)(3).

H. Information Obtained Prior to Effective Date of Rules

A covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of the HIPAA Privacy Rules pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction. § 164.532(b).

---

[7]"Parent" is used to refer to natural parent, guardian, or other person acting *in loco parentis.*

I. Other General Restrictions on Use or Disclosure

Disclosures of Protected Health Information are subject to restrictions made by agreement on scope and methods of disclosure (§§ 164.502(h); 164.522(b)) and to the uses listed in required notices. § 164.502(i).

IV. Treatment, Payment and Health Care Operations

OHIO LAW PRE-EMPTION

RC 5126.044 requires individual's consent for treatment and release from individual to disclose any PHI (other than the individual's identity if necessary for treatment or payment) to entity other than DD Board or Provider in preparation of any ISP. RC 5126.044(B). In general, a Release is required for contacts outside covered entity.

A covered entity may, without required consent or authorization:

1. use or disclose protected health information for its own treatment[8], payment[9], or health care operations[10];

2. use or disclose protected health information for the treatment activities of any health care provider;

3. disclose protected health information to another covered entity or any health care provider for the payment activities of the entity that receives the information;

4. disclose protected health information to another covered entity for the health care operations activities of the entity that receives the information, if

   (a) if each entity either has or had a relationship with the individual who is the subject of the information, and

   (b) the protected health information pertains to such relationship, and

---

[8]See section IV.B.

[9]See section IV.C.

[10]See section IV.D.

(c) the disclosure is:

(i) For quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, case management and care coordination, conducting training programs, and accreditation, licensing, or credentialing activities; or

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

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

Disclosures pursuant to the above provisions may be made to or by a business associate of a covered entity. Covered entities must follow all requirements for authorization and notice. The rules related to treatment, payment and health care operations will be treated separately below.

§ 164.506

A. Voluntary Consent

A covered entity is not required to obtain an individual's consent prior to using and disclosing information about him or her for treatment, payment, and health care operations. A covered entity may agree to seek consent, but obtaining a consent voluntarily does not permit a use or disclosure of protected health information when an authorization is required. § 164.506.

Whether or not a covered entity seeks consent, the entity must follow the notice requirements and disclose only minimum necessary information.

Individuals retain the right to request restrictions, subject to the consent of the covered entity; agreements on restrictions must be observed. § 164.502(c).

B. Treatment

OHIO LAW PRE-EMPTION

State law pre-empts. RC 5126.044(B) requires consent for any disclosure of personal records outside of treatment team except for the identity of the individual when such a disclosure is necessary for treatment.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including

1. the coordination or management of health care by a health care provider with a third party;
2. consultation between health care providers relating to a patient; or
3. the referral of a patient for health care from one health care provider to another. § 164.501.

C. Payment

OHIO LAW PRE-EMPTION

State law pre-empts. State law does not permit disclosure of information or records on an individual for payment purposes without a release. Compliance can be achieved by including consent for payment as part of eligibility application or payment authorization attached to ISP. Only the identity of the individual may be released if necessary for payment purposes.

Payment as defined in § 164.501 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.

These payment activities include, but are not limited to:

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

2. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

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

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

5. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

6. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

   (A) Name and address;
   (B) Date of birth;
   (C) Social security number;
   (D) Payment history;
   (E) Account number; and
   (F) Name and address of the health care provider and/or health plan.

D. Health Care Operations

Health care operations as defined in §164.501 are the listed activities undertaken by the covered entity that maintains the protected health information (i.e., one covered entity may not disclose protected health information for the operations of a second covered entity); a covered entity may use any protected health information it maintains for its operations (e.g., a plan may use protected health information about former enrollees as well as current enrollees). The concept of "health care operations" was included to clarify the activities considered to be "compatible with and directly related to" treatment and payment and for which protected health information could be used or disclosed without the more stringent requirements of individual authorization. 65 Fed. Reg. 82490.

The following activities are included in the definition of health care activities.

1. Any of the following QA/QI related activities:

   (a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that

the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;[11]

(b) Population-based activities relating to improving health or reducing health care costs;
(c) protocol development;
(d) case management and care coordination;
(e) contacting of health care providers and patients with information about treatment alternatives; and
(f) related functions that do not include treatment.

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

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

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

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

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

---

[11] A study with the purpose of obtaining generalizable knowledge would meet the rule's definition of research, and use or disclosure of protected health information would have to meet the requirements of §§ 164.508 or 164.512(i). Thus, studies may be conducted as a health care operation if development of generalizable knowledge is not the primary goal. However, if the study changes and the covered entity intends the results to be generalizable, the change should be documented by the covered entity as proof that, when initiated, the primary purpose was health care operations. 65 Fed. Reg. 82490.

(a) Management activities relating to implementation of and compliance with the requirements of this subchapter;
(b) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer;
(c) Resolution of internal grievances;
(d) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(e) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

V. Authorizations

A. General Rules for Authorizations

Covered entities are required to obtain an authorization for uses and disclosures of protected health information, unless the use or disclosure is required or otherwise permitted by the Rule (e.g., disclosures for treatment, payment, or health care operations summarized in section IV, reporting child abuse, section VII.D, disclosures to law enforcement, section VII.G).

Covered entities may use only authorizations that meet the requirements of § 164.508(b), summarized at sections V.B and V.C. Any such use or disclosure will be lawful only to the extent the use or disclosure is consistent with the terms of such authorization.

A voluntary consent document will not constitute a valid permission to use or disclose protected health information for a purpose that requires an authorization under the Rule. § 164.508(a).

Covered entities must document and retain signed authorizations for six years after the authorization was created or last in effect, whichever is later. §§ 164.508(b)(6), 164.530(j). The covered entities must provide the individual with a copy of the authorization. §§ 164.508(c)(4).

OHIO LAW PRE-EMPTION

The DD Board must retain all records and forms, including, but not limited to ISPs, necessary to fully disclose the extent of services provided and related business transactions for a period of seven years from the date of receipt of payment, or for six years after any initiated audit is completed and adjudicated, whichever is longer. Similar requirements apply to ICF/MR and waiver records.

B. Essential Elements

A valid authorization must be written in plain language (§ 164.508(c)(3)) and include at least all of the following core elements and statements:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

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

4. A description of each purpose of the use or disclosure. When individuals initiate an authorization for their own purposes, the purpose may be stated as "at the request of the individual."

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

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

7. In addition to these core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(a) A statement of the individual's right to revoke the authorization in writing and either

(i) the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization; or

(ii) a reference to the covered entity's notice if these exceptions are listed in the notice summarized in section IX.

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

(i) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization, if applicable;[12] or

(ii) The consequences to the individual of a refusal to sign the authorization when the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(c) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule.

§ 164.508(c)(1) and (2).

If the authorization is for marketing purposes and the covered entity will receive either direct or indirect compensation, the authorization must state that the covered entity will receive remuneration. § 164.508(a)(3)(ii).

C. When Authorization Form is not Valid

An authorization is not valid when:

1. The expiration date has passed or the expiration event is known by the covered entity to have occurred;

---

[12]See section V.E on when an entity can condition treatment, enrollment in the health plan, or eligibility for benefits on signing an authorization.

2. Any required element is missing or has not been filled out, if required;

3. The authorization is known by the covered entity to have been revoked;

4. The authorization has been improperly combined with another document (see section V.D);

5. The covered entity has violated the rules on making the authorization a condition. See section V.E.

6. Any material information in the authorization is known by the covered entity to be false.

§ 164.508(b)(2).

D. Compound Authorizations

An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

1. An authorization for the use or disclosure of protected health information 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 protected health information for such research or a consent to participate in such research.

2. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

3. An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section, except when a covered entity has conditioned[13] the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations.

§ 164.508(b)(3).

---

[13]See section V.E on when an entity can condition treatment, enrollment in the health plan, or eligibility for benefits on signing an authorization.

E. 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:

1. A covered health care provider may condition the provision of research-related treatment on provision of a valid authorization;

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

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

   (b) The authorization is not for a use or disclosure of psychotherapy notes (see discussion on such notes in section VIII.A).

3. A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

§ 164.508(b)(4).

F. Revoking Authorizations

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

1. The covered entity has taken action in reliance thereon; or

2. 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.

§ 164.508(b)(5).

VI. When a Person Must Be Allowed to Agree or Object

A. General Rules

A covered entity may use or disclose protected health information without authorization provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure in accordance with this section. § 164.510.

B. Facility Directories

Unless an individual objects, a Health Care Provider may develop a directory which includes the individual's name, location in the covered health care provider's facility, and condition described in general terms that does not communicate specific medical information about the individual, and religious affiliation. This information may be disclosed to clergy and to persons who ask for the individual by name. § 164.510(a)(1).

A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures listed above. § 164.510(a)(2).

If an individual cannot be given the opportunity to object because of the individual's incapacity or emergency circumstances, a covered health care provider may use or disclose some or all of the information listed above for the facility's directory, if such disclosure is:

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

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

The individual must be given the opportunity to object as soon as reasonably practicable. § 164.510(a)(3).

C. Disclosure to Persons Involved in Individual's Care

OHIO LAW PRE-EMPTION

RC 5126.044 requires individual's consent for treatment and release from individual to disclose any PHI (other than the individual's identity if necessary for treatment or payment) to entity other than DD Board or Provider in preparation of any ISP. RC 5126.044(B). In general, a Release is required for contacts outside covered entity.

1. A covered entity may, in accordance with the rules summarized below, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. § 164.510(b)(1)(i).

2. A covered entity may, in accordance with the rules summarized below, use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. § 164.510(b)(1)(ii).

3. If the individual is present or available prior to the permitted disclosures under this section VI.C , and has the capacity to make decisions, the covered entity may use or disclose the protected health information if it:

   (a) Obtains the individual's agreement;
   (b) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
   (c) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure. § 164.510(b)(2).

4. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on

behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information. § 164.510(b)(3).

5. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures to involved persons described in section VI.C.2. The requirements in sections VI.C.3 and VI.C.4 apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances. § 164.510(b)(4).

VII. What Information Can Be Obtained Without Authorization or Opportunity to Object

A. General

This section covers circumstances when there is no requirement for authorization or opportunity to object. § 164.512. The summary covers only selected issues which are likely to affect DD Boards.

B. Disclosures required by law

A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. The entity must comply with limits on disclosure summarized in sections VII.E, VII.F, and VII.G below. § 164.512(a).

C. Disclosures to avert a serious threat to health or safety

1. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and is either

   (a) to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

   (b) Is necessary for law enforcement authorities to identify or apprehend an individual:

(i) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(ii) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody. § 164.512(j).

2. Disclosure to law enforcement is not permitted under VII.C.1.(b)(i) if the information was obtained in the course of treatment, counseling, or therapy to affect the propensity to commit the criminal conduct that is the basis for the disclosure or if the information was obtained through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy to affect the propensity to commit criminal conduct. § 164.512(j)(2).

3. Disclosure from a person admitting participation in a violent crime is limited to the statement of participation and the following information:

(a) Name and address;
(b) Date and place of birth;
(c) Social security number;
(d) ABO blood type and Rh factor;
(e) Type of injury;
(f) Date and time of treatment;
(g) Date and time of death, if applicable; and
(h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos. § 164.512(j)(3); 164.512(f)(2)(i).

4. A covered entity that uses or discloses protected health information under this section is presumed to have acted in good faith if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority. § 164.512(j)(4).

D. Disclosures about child abuse

State law on disclosures of child abuse must be followed without restriction. § 164.512(a)(1); 164.512(b)(1)(ii).

E. Disclosures about adult victims of abuse, neglect or domestic violence

1. Except for reports of child abuse or neglect permitted in section VII.D, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence. § 164.512(c)(1). Disclosures under this section can be made only if:

   (a) Disclosure can be made only to the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or

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

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

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

      (ii) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure. § 164.512(c)(1).

2. A covered entity that makes a disclosure under this section must promptly inform the individual that such a report has been or will be made, unless:

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

   (b) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person

would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment. § 164.512(c)(2).

F. Disclosures for judicial and administrative proceedings

1. Court orders: A covered entity must always comply with a lawful order, but only in accordance with the express terms of the order. § 164.512(e)(1)(i).

2. Subpoena, discovery request or other lawful process: a covered entity may comply with such legal requests only if:

   (a) The covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice[14] of the request; or

   (b) The covered entity receives satisfactory assurance[15] from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order. § 164.512(e)(1)(ii).

G. Disclosures for law enforcement activities

1. General: Disclosure is permitted under any of the following circumstances:

   (a) when required by law including laws that require the reporting of certain types of wounds or other physical injuries;
   (b) in response to valid court orders, subpoenas, summons to grand jury proceedings or properly issued demands of administrative bodies. § 164.512(f)(1).

2. Identification and location of a suspect: A covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that the covered entity may disclose only the following information:

---

[14]Elements of required notice are in § 164.512(e)(1)(iii).

[15]The rules define conditions for demonstrating "satisfactory assurance" and conditions for a "qualified protective order". § 164.512(e)(1)(iv).

(a) Name and address;
(b) Date and place of birth;
(c) Social security number;
(d) ABO blood type and Rh factor;
(e) Type of injury;
(f) Date and time of treatment;
(g) Date and time of death, if applicable; and
(h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos. § 164.512(f)(2)(i).

Unless otherwise required by law, a covered entity may not disclose 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. § 164.512(f)(2)(ii).

3. Victim of crime: Information about a victim may be given to assist in finding the perpetrator of a crime if

(a) the victim agrees; or
(b) if the victim is unable to agree because of incapacity,
    (i) the law enforcement official represents that the information is essential and will not be used against the victim and
    (ii) the entity determines that disclosure is in the best interest of the victim. § 164.512(f)(3).

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

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

6. Reporting Crime in Emergencies:

(a) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health

information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(i) The commission and nature of a crime;
(ii) The location of such crime or of the victim(s) of such crime; and
(iii) The identity, description, and location of the perpetrator of such crime.

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

H. Disclosures for health oversight activities

1. General: Information may be used by a health oversight agency or disclosed to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

   (a) The health care system;
   (b) Government benefit programs for which health information is relevant to beneficiary eligibility;
   (c) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
   (d) Entities subject to civil rights laws for which health information is necessary for determining compliance. § 164.512(d)(1), (4).

2. A health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

   (a) The receipt of health care;
   (b) A claim for public benefits related to health; or
   (c) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.
   § 164.512(d)(2).

VIII. Special Requirements

A. Psychotherapy Notes

The HIPAA Privacy Rules give special protection to psychotherapy notes. Psychotherapy notes are defined as

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

§ 164.501.

A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

1. Authorization is not needed for the following treatment, payment, or health care operations:

   (a) Use by the originator of the psychotherapy notes for treatment;

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

   (c) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual. § 164.508(a)(2)(i).

2. Authorization is not needed for certain oversight and monitoring activities or to prevent danger to third parties. § 164.508(a)(2)(ii).

3. Authorizations are not required during the transition phase. § 164.508(a)(2).

B. De-identified Protected Health Information

Once personally identifiable information has been removed from Protected Health Information, the information is not subject to the HIPAA Privacy Rules. The rules do apply to any codes which can identify the data and to the data if personally identifiable information is restored. § 164.502(d).

A record has been "de-identified" when health information does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. § 164.514(a). The rule lists which elements must be removed to be "de-identified"; the list requires removal of birth dates and parts of zip codes, depending on the size of the population within the zip code. § 164.514(b).[16]

---

[16]Elements are listed at § 164.514(b)(2):

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code except as permitted by

C. Limited Data Sets

1. General

The HIPAA rules create the concept of a "limited data set" which allows for disclosure of limited information for research, public health, or health care operations purposes if the covered entity (1) uses or discloses only a "limited data set" as defined in the rules and (2) obtains from the recipient of the limited data set a "data use agreement". § 164.514(e).

The covered entity does not need to include disclosures of protected health information in limited data sets in any accounting of disclosures provided to the individual. § 164.528(a)(1)(viii).

2. Scope of Limited Data Set

The rules do not delineate the data that can be released through a limited data set. Rather, the HIPAA Rule specifies that certain information be removed regarding the individual, the individual's relatives, employers, or household members. The information that must be removed to qualify as a limited data set include all of the following:

(a) Name;
(b) street address (renamed postal address information, other than city, State and zip code)[17];
(c) telephone and fax numbers;
(d) e-mail address;
(e) social security number;
(f) certificate/license numbers;
(g) vehicle identifiers and serial numbers;
(h) URLs and IP addresses;
(i) full face photos and any other comparable images.
(j) Medical record numbers, health plan beneficiary numbers, and other account numbers;
(k) device identifiers and serial numbers; and

(c) of the rules and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

[17]Note that limited data sets can include city, State and zip code. This same information must be removed in order to de-identify the data in accordance with § 164.514(b)(2).

(l) biometric identifiers, including finger and voice prints.

§ 164.514(e)(2). A covered entity that wants to subcontract the task of creating a Limited Data Set from protected health information must first establish a business associate relationship with the person or entity which will do the work. § 164.514(e)(3)(ii).

3. Data Use Agreements

Use of a Limited Data Set requires a Data Use Agreement with the intended recipient. The agreement must

(a) establish the permitted uses and disclosures of such information by the recipient, consistent with the purposes of research, public health, or health care operations;

(b) limit who can use or receive the data;

(c) require the recipient to agree not to re-identify the data or contact the individuals;

(d) require that the recipient use appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the Rule and the data use agreement, or as required by law;

(e) require that the recipient will report any unauthorized use or disclosure of which the recipient has become aware;

(f) Require that the recipient impose the same restrictions and requirements on any subcontractors or agents.

§ 164.514(e)(4)(ii).

4. Compliance

A covered entity is not in compliance with these standards if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation.

If steps are unsuccessful, the covered entity must discontinue disclosure of protected health information to the recipient under the Data Use Agreement and report the problem to the Secretary.

A recipient of a Limited Data Set under a Data Use Agreement is not in compliance with these standards if the recipient violates the Data Use Agreement. § 164.514(e)(4)(iii).

IX. Notice of Privacy Practices

A. General

In general, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. § 164.520(a).

B. Content of the Notice

The notice must conform to the requirements of the rule and include the elements summarized below. § 164.520(b). The description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by HIPAA rules and other applicable law. § 164.520(b). The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected. § 164.520(b)(3). The required notice elements are as follows:

1. A statement as a header or otherwise prominently displayed which states that, "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."

2. A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by HIPAA rules to make for each of the following purposes: treatment, payment, and health care operations.

3. A description of each of the other purposes for which the covered entity is permitted or required by HIPAA rules to use or disclose protected health information without the individual's written authorization.

4. Those areas which are subject to more restrictive state requirements.

5. 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.

6. If applicable, a separate statement that:

   (a) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;
   (b) The covered entity may contact the individual to raise funds for the covered entity; or
   (c) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

7. A statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

   (a) The right to request restrictions on certain uses and disclosures of protected health information as provided in the rules including a statement that the covered entity is not required to agree to a requested restriction;
   (b) The right to receive confidential communications of protected health information as applicable;
   (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 of an individual, including an individual who has agreed to receive the notice electronically to obtain a paper copy of the notice from the covered entity upon request.

8. A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;

9. A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

10. A statement that the covered entity has the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

11. The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

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

13. 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.

14. If the covered entity has opted to impose further limits, these limits must be summarized with a statement that the limits may be altered.

§ 164.520(b).

C. Providing notice

In general, notice must be made available upon request and at times specified below § 164.520(c):

1. Health Plans must give notice to all persons at time of enrollment and within 60 days of a material revision. Notice of the availability of notice and how to obtain notice must be given at least every three years after enrollment. § 164.520(c)(1).

2. Health Care Providers must give a copy of the notice no later than the date of first service delivery to all persons with whom there is a direct treatment relationship.

   (a) In an emergency, notice may be given as soon as practicable.

   (b) Where there is a physical service delivery site, the Provider must have the notice available at the service delivery site for individuals to request to take with them and post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice.

   (c) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision. § 164.520(c)(2).

3. Notice may be posted on a web-site and delivered by e-mail under specified circumstances. § 164.520(c)(3).

4. Documentation: A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity. § 164.520(e).

D. Acknowledgment of Receipt of Notice

A covered direct treatment provider is required to make a good faith effort to obtain a written acknowledgment of receipt of the notice, including receipt of an electronic notice. Except in an emergency, the acknowledgment must be received no later than the date of first service delivery, including service delivered electronically, that is, at the time the notice is required to be provided. In an emergency, acknowledgment must be obtained as soon as practicable after the emergency. § 164.520(c)(2).

If an individual refuses to sign or otherwise fails to provide an acknowledgment, a covered health care provider is required to document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained. § 164.520(c)(2).

There are no formal requirements for the written acknowledgment, including no requirement for the individual's signature on the acknowledgment. The Department of HHS does not, however, consider oral acknowledgment by the individual to be either a meaningful or appropriate manner by which a covered health care provider may implement these provisions. 67 Fed. Reg. 53240.[18]

X. Voluntary Restrictions

An individual must have the right to request additional restrictions on access. The covered entity is not required to comply, but if the entity chooses to do so, then the entity must abide by those restrictions, except in an emergency or other situations where disclosure is legally required. An entity may remove a restriction either by agreement or unilaterally, if specified procedures are followed. Unilateral removal of a restriction can be applied prospectively only. § 164.522.

An individual may request, subject to specified conditions in the rules, that confidential information be conveyed by the covered entity to the individual through alternative means or at alternative locations. § 164.522(b).

---

[18]References to volume 67 of the Federal Register are to 67 Fed. Reg. No. 157 Part V August 14, 2002, pp. 53182 - 53273.

XI. Access to Records by the Individual

A. General

OHIO LAW PRE-EMPTION

State law pre-empts HIPAA exceptions. There are no limits in state law to an individual's access. RC 5126.044(D)(1)

In general, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

1. Psychotherapy notes;
2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
3. Protected health information covered by Clinical Laboratory Improvements Amendments of 1988.

§ 164.524(a)(1).

B. Unreviewable grounds for denial of access

A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances:

1. The protected health information is excepted from the right of access under section XI.A above.

2. A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

3. An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may

be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

4. An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

5. An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

§ 164.524(a)(2).

C. Reviewable grounds for denial of access

OHIO LAW PRE-EMPTION

State law pre-empts HIPAA exceptions. There are no limits in state law to an individual's access, whatever the format of the information, including electronic or paper records. RC 5126.044(D)(1).

A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed under the rules in the following circumstances:

1. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

2. The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

3. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably

likely to cause substantial harm to the individual or another person. § 164.524(a)(3).

D. Procedure for review of denial

If access is denied on a ground which allows for review, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official. § 164.524(a)(4).

E. Procedure and Deadlines for Response

1. A covered entity may require that a request be in writing.

2. In general, once a request is made, the entity must respond no later than 30 days after receipt of the request in accordance with the following procedures (§ 164.524(b)):

   (a) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested.

   (b) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial which conforms to the requirements of the rules.

3. If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action described in the previous paragraph by no later than 60 days from the receipt of such a request.

4. An entity may extend a deadline by not more than 30 days. The entity must provide the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request.

F. Procedures when access is granted

If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

1. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

2. The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

3. The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

   (a) The individual agrees in advance to such a summary or explanation; and
   (b) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

4. The covered entity must provide the access as requested by the individual in a timely manner as summarized above, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

5. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

   (a) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;
   (b) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
   (c) Preparing an explanation or summary of the protected health information, if agreed to by the individual as summarized above.

§ 164.524(c).

G. Procedures when access is denied

If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

1. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

2. The covered entity must provide a timely, written statement of denial to the individual. The denial must be in plain language and contain:

   (a) The basis for the denial;
   (b) If applicable, a statement of the individual's review rights including a description of how the individual may exercise such review rights; and
   (c) A description of how the individual may complain to the covered entity or to the Secretary pursuant to the rules.

3. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

4. If the individual has requested a review of a denial under this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards summarized in section XI.C. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

§ 164.524(d).

H. Documentation

A covered entity must document the following and retain the documentation as required by the rules:

1. The designated record sets that are subject to access by individuals; and

2. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.524(e).

XII. Right to Amend Records

A. General

Subject to the rules summarized below, an individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set. § 164.526(a)(1).

B. Denial of amendment: Basis

A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

1. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

2. Is not part of the designated record set;

3. Would not be available for inspection under rules summarized at section XI; or

4. Is accurate and complete.

§ 164.526(a)(2).

C. General Procedures

1. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

2. The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request. The covered entity may extend the time for such action by no more than 30 days, provided that the covered entity

provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request. The notice must be given before the expiration of the 60 day time limit.

§ 164.526(b).

D. Procedures if amendment is accepted

If the covered entity accepts the requested amendment, in whole or in part, the covered entity must make the appropriate amendment, and inform the individual and other persons or entities who have had access to the information. § 164.526(c).

E. Denial of amendment: Process

1. If an amendment is denied, the covered entity must give written notice in plain language which includes the following:

   (a) The basis for the denial, in accordance with section XII.B;

   (b) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

   (c) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

   (d) A description of how the individual may complain to the covered entity or the Secretary under the rules. The description must include the name, or title, and telephone number of the contact person or office. § 164.526(d)(1).

2. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement. § 164.526(d)(2).

3. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement § 164.526(d)(3).

4. Records must allow review of the statements of disagreement and rebuttals. § 164.526(d)(4). Future disclosures of covered records must include relevant amendments and rebuttals. § 164.526(d)(5).

F. Other entities

A covered entity that is informed by another covered entity of an amendment to an individual's protected health information must amend the protected health information in designated record sets. § 164.526(e).

G. 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 rules. § 164.526(f).

XIII. Accounting of Disclosures

A. General

The rules for accounting have changed in Ohio and Federal law in 2009. Although Federal law continues to require accounting for disclosures, Ohio law no longer requires any such accounting under RC 5126.044.

Under new Federal requirements, PHI used or maintained in electronic format is subject to the revised accounting requirements. ARRA, § 13405(c). Unless the individual has signed an authorization, the following types of disclosure require an accounting:

1. Treatment, payment and health care operations for three years prior to the request
2. Other disclosures for six years prior to the request including, for example,
   (a) Between BA and covered entity
   (b) Health oversight
   (c) Reports of MUIs outside of the covered entity
   (d) other disclosures not specifically exempted by 164.528

Accounting requirements now apply to both covered entities and business associates. ARRA, § 13404(a). The BA agreement must define the process for responding to requests for accountings. ARRA, § 13405(c)(3).

B. When Accounting Rules will Apply

If the record exists on or before January 1, 2009, the new accounting requirements will apply to disclosures made from that record on or after January 1, 2014. ARRA, § 13405(c)(4)(A).

If the record exists after January 1, 2009, the new accounting requirements will apply to disclosures made from that record on or after the later of January 1, 2011 or the date the covered entity acquires the electronic health record.[19] ARRA, § 13405(c)(4)(B).

C. Procedure for Accountings

Accountings must be given within the time specified by the rules. § 164.528(c).

In general, the content of the accounting must include the following for each disclosure:

1. The date of the disclosure;
2. The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
3. A brief description of the protected health information disclosed; and
4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:
   (a) A copy of the individual's written authorization under the rules; or
   (b) A copy of a written request for a disclosure, if any.

Multiple disclosures of the same protected health information to the same person or entity for a single purpose and disclosures for research are subject to different requirements.

§ 164.528(b).

D. Exceptions

The following disclosures are not subject to the accounting requirements, if carried out in accordance with HIPAA Privacy Rules:

---

[19] The Secretary may set a later date for compliance with these accounting requirements. ARRA, § 13405(c)(4)(C).

1. To carry out treatment, payment and health care operations, except that PHI maintained electronically is subject to accounting for three years prior to the request. See section XIII.A;
2. To individuals of protected health information about them;
3. Incident to a use or disclosure otherwise permitted or required by the HIPAA Privacy Rules;
4. Pursuant to an authorization;
5. For the facility's directory or to persons involved in the individual's care or other notification purposes;
6. For national security or intelligence purposes;
7. To correctional institutions or law enforcement officials;
8. As part of a limited data set; or
9. That occurred prior to the compliance date for the covered entity.

§ 164.528(a)(1).

XIV. Business Associates

A. What Is a Business Associate Relationship

A Business Associate relationship occurs when the right to use or disclose the protected health information belongs to the covered entity, and another person or entity (the business associate) is using or disclosing the protected health information (or creating, obtaining and using the protected health information) to perform a function or activity on behalf of the covered entity. § 160.103.

Providing specified services to a covered entity creates a business associate relationship if the provision of the service involves the disclosure of protected health information to the service provider. Examples of services creating a business associate relationship include legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services. § 160.103.

An entity participating in an Organized Health Care Arrangement may exchange information with other participating entities without creating a business associate relationship. § 160.103.

An accreditation organization (such as CARF or JCAHO) for a program of the DD Board is a business associate of the DD Board if the accreditation organization reviews PHI as part of the accreditation process. § 160.103.

In our opinion, the accreditation activities of DoDD under RC § 5126.081 are health oversight activities which do not require a business associate contract. RC § 5126.081 requires accreditation "to ensure that the boards are in compliance with federal and state statutes and rules".

The DoDD is not a business associate of a DD Board when the DoDD collects PHI from the DD Board to determine eligibility or enrollment for a government program such as Medicaid.

B. Implications of Business Associate Relationship

OHIO LAW PRE-EMPTION

RC 5126.044 requires individual's consent for treatment and release from individual to disclose any PHI (other than the individual's identity if necessary for treatment or payment) to entity other than DD Board or Provider in preparation of any ISP. RC 5126.044(B). State law pre-empts HIPAA on release to business associates unless business associate can be considered an employee of the DD Board.

A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. § 164.502(e)(1)(i).

C. General Duties of a Business Associate

Under § 13401 and 13404(a) of the ARRA, Business Associates are generally required to comply with the same requirements as a covered entity for following Privacy requirements of HIPAA and for implementing Administrative Safeguards under § 164.308, Physical Safeguards under § 164.320, Technical Safeguards under § 164.312 and Policy, Procedures and Documentation Requirements under § 164.316.

Business Associates have an affirmative duty to report violations by a covered entity which are related to the BA agreement. § 164.504(e)(1)(ii); ARRA § 13404(b).

A Business Associate must, following the discovery of a breach of unsecured protected health information, notify the Covered Entity of such breach. §164.410. For further details see section XX.

The covered entity and Business Associate must include provisions in the BA Agreement which defines responsibility for accounting of disclosures. ARRA § 13405(c)(3).

Business Associates are subject to the same civil and criminal penalties as a covered entity. ARRA § 13404 (a) and (c)). See section XXI, XXI.

D. Establishing a Business Associate Relationship

A covered entity may create a business associate relationship with another private entity through a contract which meets the requirements summarized below in section XIV.E. Comparable relationships between governmental entities may be established through a Memorandum of Understanding or other similar written arrangement.

E. Contracts with Business Associates

A covered entity must document satisfactory assurances that the business associate will safeguard protected health information. These assurances must be documented through either a written contract or other written agreement or arrangement with the business associate. § 164.502(e)(2). Such contracts or arrangements must meet the requirements of § 164.504(e) and must do all of the following:

1. Define permitted and required uses and disclosures of such information by the business associate.

2. Prohibit the business associate from using or further disclosing the information in a manner that would violate HIPAA Privacy Rules, if done by the covered entity, except that:

    (a) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate; and

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

3. Require that the business associate does all of the following:

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

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

(c) Ensure that any agents or subcontractors of the business associate agree to the same restrictions and conditions that apply to the business associate;

(d) Make available protected health information to individuals requesting access to records in accordance with rules summarized in section XI;

(e) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with rules summarized in section XII;

(f) Make available the information required to provide an accounting of disclosures in accordance with rules summarized in section XIII;

(g) Allow access to all data which is the subject of the contract to the Secretary of HHS for purposes of determining the covered entity's compliance with HIPAA Privacy Rules; and

(h) At termination of the contract, if feasible, return or destroy all protected health information covered by the contract or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

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

5. May permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

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

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

6. May permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in previous section XIV.E.5, if the disclosure is required by law; or

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

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

§ 164.504(e)(2), (4).

F. Business Associate Relationships between Governmental Entities

OHIO LAW PRE-EMPTION

RC 5126.044 requires individual's consent for treatment and release from individual to disclose any PHI (other than the individual's identity if necessary for treatment or payment) to entity other than DD Board or Provider in preparation of any ISP. RC 5126.044(B). State law pre-empts HIPAA on release to business associates including other governmental entities.

Governmental entities which are acting as business associates (e.g., COGs) may enter into Memoranda of Understanding or other comparable arrangements which are sufficient under Ohio Law to establish a business associate arrangement (e.g., COG). The MOU or agreement must comply with legal requirements for the relationship or, if there are no legal directives, include all

of the elements in section XIV.E above, except that the termination provisions may be altered to correspond with applicable state law.[20] § 164.504(e)(3)

A covered entity must disclose information to another governmental entity acting in a business associate role, if disclosure is required by law. The covered entity should attempt to obtain appropriate assurances; if assurances cannot be obtained, the covered entity must document the attempts and the reasons why the assurances could not be obtained. § 164.504(e)(3)(ii).

To the extent that a group of governmental entities, such as a Family and Children First Council, is acting as an organized health care arrangement (see footnote 5) there is no need for an MOU.

G. Enforcement of Business Associate Contracts

A Business Associate is in violation of HIPAA Privacy Rules if the Business Associate breaches any of the rules or violates a contract which includes the provisions summarized above in section XIV.E. Sanctions are summarized in section 56.

A covered entity is not in compliance with these standards if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate contract or agreement, unless the covered entity took reasonable steps to cure the breach or end the violation.

If steps are unsuccessful, the covered entity must discontinue disclosure of protected health information to the business associate under the business associate contract or agreement and report the problem to the Secretary.

§ 164.504(e)

---

[20]For example, a COG may be established by following the requirements of Chapter 167 of the Ohio Revised Code ("RC") and, once established, the exchange of PHI may occur under business associate relationship rules. If Family and Children First Councils want to exchange PHI, however, a business associate agreement must be established which meets the requirements of § 164.504(e)(3) since there are no state laws which govern the agreements between entities which form a FCFC.

XV. Administrative Requirements

A. Personnel Designations

A covered entity must designate and document:

1. A privacy official responsible for the development and implementation of the policies and procedures of the entity.

2. A contact person or office responsible for:
   (a) receiving complaints under this section and
   (b) Providing further information about matters covered by the required notice.

§ 164.530(a).

B. Training

1. General: A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by HIPAA rules, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity. § 164.530(b)(1). All training must be documented. § 164.530(b)(2)(ii).

2. Timing:

   (a) All existing employees must be trained by no later than the compliance date for the covered entity.

   (b) New employees must be trained within a reasonable time after hiring.

   (c) Employees whose functions are affected by a material change in the policies or procedures must be trained within a reasonable period of time after the material change becomes effective. § 164.530(b)(2)(i).

C. Safeguards

A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. Safeguards must be adequate to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the HIPAA rules. § 164.530(c).

D. Complaints

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by HIPAA rules or its compliance with such policies and procedures or the requirements of HIPAA rules. Complaints and their disposition, if any, must be documented. § 164.530(d).

E. Sanctions

A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of HIPAA rules. Sanctions may not be applied to whistleblowers (as defined in § 164.502(j)) or in a manner which would be construed as intimidation or retaliation as summarized in section XV.G.2. § 164.530(e).

F. Mitigation

A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of HIPAA rules by the covered entity or its business associate. § 164.530(f).

G. Prohibition against retaliation or intimidation

A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by HIPAA rules, including the filing of a complaint under this section;

2. Any individual or other person for:

   (a) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;
   (b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
   (c) Opposing any act or practice made unlawful by HIPAA rules, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of HIPAA rules.

§ 164.530(g).

H. Prohibition against waiver of rights

A covered entity may not require individuals to waive their rights to file a complaint with the Secretary of HHS or other rights under the HIPAA rules as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits. § 164.530(h).

I. Policies and procedures

1. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of HIPAA rules. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of HIPAA rules. § 164.530(i)(1).

2. A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart. The change will apply to existing protected health information only if the covered entity has reserved the right to do so in its original notice. Otherwise the changes will apply only to protected health information created or received after the effective date of the notice. The covered entity must document material changes in policies and notices which reflect such changes. § 164.530(i)(2-4).

3. The covered entity must give notice of all material changes and alter existing notices to reflect changes in the law. § 164.530(i)(3).

4. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice provided that the policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and is properly documented prior to the effective date of the change. § 164.530(i)(2)(iii); § 164.530(i)(5).

XVI. Rules for Various Organizational Configurations

A. Hybrid Entities

A covered entity may elect to be considered a hybrid entity if the business activities of the entity include both covered and non-covered functions[21]. A hybrid entity must designate one or more of its functions as a health care component. A health care component is an activity which, if operating independently, would be a covered entity. Health care components may also include a component only to the extent that it performs either:

1. covered functions, or
2. activities that would make such a component a business associate of a component that performs covered functions if the two were separate entities.

§ 164.504(a), (c)(3)(iii).

---

[21]There is no need to determine whether the non-covered functions are primary.

A hybrid entity is required to create adequate separation, in the form of firewalls, between the health care component(s) and other components of the entity. Transfer of protected health information held by the health care component to other components of the hybrid entity continues to be a disclosure under the Privacy Rule, and, thus, will generally require an authorization.

Covered entities that choose not to designate health care component(s) are subject to the Privacy Rule in their entirety.

Even if a covered entity does not choose to be a hybrid entity, and therefore is not required to erect firewalls around its health care functions, the entity still only is allowed to use protected health information as permitted by the Privacy Rule, for example, for treatment, payment, and health care operations.

Additionally, the covered entity is still subject to minimum necessary restrictions under §§ 164.502 and 164.514(d), and, thus, must have policies and procedures that describe who within the entity may have access to the protected health information. Under these provisions, workforce members may be permitted access to protected health information only as necessary to carry out their duties with respect to the entity's covered functions. For example, the health insurance line of a multi-line insurer is not permitted to share protected health information with the life insurance line for purposes of determining eligibility for life insurance benefits or any other life insurance purposes absent an individual's written authorization.

B. Affiliated Covered Entities

Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of HIPAA rules, if all of the covered entities designated are under common ownership or control.[22] § 164.504(d)(1), (2). Once affiliated in accordance with HIPAA Privacy Rules, the affiliated covered entity's use and disclosure of protected health information must comply with the applicable requirements of the HIPAA Privacy Rules. § 164.504(d)(3).

---

[22]*Common control* exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. § 164.504(a).

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity. § 164.504(a).

C. Covered Entity with 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 applicable standards, requirements, and implementation specifications of the HIPAA Privacy Rules.

A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed. § 164.504(g).

D. Rules Applicable to Health Care Clearinghouses

When a Health Care Clearinghouse[23] creates or receives Protected Health Information in a role which is other than as a Business Associate[24] of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of the HIPAA Privacy Rules. § 164.500(b)(2).

When a Health Care Clearinghouse creates or receives Protected Health Information as a business associate, the clearinghouse must meet the following standards:

1. The general rules in § 164.502, summarized in section II.D, except that the clearinghouse can only use protected health information in accordance with the terms of the business associate contract;
2. The rules for organizational requirements in § 164.504.
3. Requirements for disclosure without authorization or opportunity to agree or object in § 164.512, except that the clearinghouse can only use protected health information in accordance with the terms of the business associate contract.

§ 164.500(b)(1).

---

[23]See definition in footnote 3.

[24]See section XIV for definition and discussion of a Business Associate.

XVII. Conflict with Existing State Requirements

In general, if there is a conflict between state and federal privacy requirements, the more restrictive rule applies. §§ 160.201 - 203.

XVIII. Notice of Breach

Effective September 23, 2009, all HIPAA Covered Entities and their Business Associates are required to provide notice in the event of a breach of unsecured protected health information (PHI). Covered Entities must notify the affected individual, the Secretary of HHS and under some circumstances even the media. Business Associates must provide notice of a breach to the Covered Entity. Failure to comply may lead to civil penalties which have been significantly increased under the ARRA revisions. Additionally civil penalties for HIPAA violations are being extended to Business Associates as well as Covered Entities.

A. Breaches subject to Notification

Under the new regulations, notification requirements apply to breaches of unsecured PHI. To determine whether notification is required, the Covered Entity or Business Associate must first determine (1) whether there is a breach, and (2) whether the breach includes unsecured PHI. If the answer to both is yes, then notification is required.

B. Definition of a Breach

A breach is the acquisition, access, use, or disclosure of PHI in an unauthorized manner which compromises the security or privacy of the PHI. §164.402.[25] The following types of breaches are expressly excluded from this definition:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner prohibited by HIPAA.

[25] For purposes of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that is part of a limited data set as defined by § 164.514(e)(2), does not compromise the security or privacy of the PHI. §164.402.

2. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same Covered Entity or Business Associate and the information is not further disclosed in a manner prohibited by HIPAA; or

3. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. § 164.402(2).

C. Definition of Unsecured PHI

Unsecured PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued and made available at http://www.hhs.gov/ocr/privacy/.[26] § 164.402. The regulations require this guidance to be updated annually. PHI which is secured as specified by the guidance will not be subject to notification in the event there is a breach of the secured PHI.

XIX. Notification Requirements Applicable to the Covered Entity

A. Notice of Breach to Individuals

A covered entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.[26] The notice must be written in plain language and to the extent possible, must include all of the following:

---

[26] The commentary notes that "unsecured PHI can include information in any form or medium, including electronic paper, or oral form." 74 Fed. Reg. 42748.

[26] §164.404(a)(1); A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity. §164.404(a)(2).

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured PHI involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a tollfree telephone number, an e-mail address, Web site, or postal address. §164.404(c).

B. Method of Notice

The Covered Entity must provide notice in one of the following three formats, depending on circumstances (§164.404(d)):

1. Written Notice

   (a) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

   (b) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to either the next of kin or personal representative of the individual.

2. Substitute Notice

In the case that contact information is not available, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in where the individual is deceased.

(a) In the case in which contact information is not available for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(b) In the case in which contact information is not available for 10 or more individuals, then such substitute notice shall:

(i) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(ii) Include a toll-free phone number that remains active for at least 90 days that an individual can call to learn whether the individual's unsecured PHI may be included in the breach.

3. Additional notice in urgent situations

In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured PHI, the covered entity may, in addition to providing written notice, contact individuals by telephone or other means, as appropriate.

C. Other Parties Required to Receive Notice

In addition to providing notice to the individual, the Covered Entity must notify the following entities:

1. Notification to the Media

For a breach of unsecured PHI involving more than 500 residents, a covered entity shall, notify prominent media outlets serving the State or jurisdiction. The content of the notice shall be the same as the notice provided to the individual. §164.406.

2. Notification to Secretary of HHS

For a breach of unsecured PHI involving more than 500 residents, a covered entity shall, notify the Secretary of HHS in the manner specified on the HHS Web site. For breaches of unsecured PHI involving less than 500 individuals, the covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide notice to the Secretary of HHS of breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site. §164.408.

D. Timeliness of Notification

In general, a Covered Entity must provide the required notice without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. §§164.404(b); 406(b); 410(b).

The Covered Entity must delay providing notice if a law enforcement official states to the Covered Entity or Business Associate that providing notice would impede a criminal investigation or cause damage to national security. If such statement is in writing and specifies the time for which a delay is required, the Covered Entity or Business Associate shall delay such notice for the time period specified by the official. If the statement is made orally, the Covered Entity or Business Associate shall document the statement, including the identity of the official making the statement, and delay the notice temporarily and no longer than 30 days from the date of the oral statement, unless the law enforcement official submits a written statement during that time. §164.412.

XX. Notification Requirements Applicable to Business Associates

A Business Associate must, following the discovery of a breach of unsecured protected health information, notify the Covered Entity of such breach. §164.410. A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business

associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate. §164.410(a)(2).

The Business Associate is subject to the requirements applicable to a Covered Entity for timeliness of notification including requirements for a delayed notification.

The notification provided by the Business Associate shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the breach.

A Business Associate must provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

XXI. Penalties

A. Private Complaints to Secretary of HHS

Any person may file a complaint with HHS raising issues of non-compliance, whether or not the person is the subject of the violation. § 160.306(a). The complaint must be in writing and filed with the Secretary within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. § 160.306(b).

B. Criminal Penalties

1. General: Criminal penalties may be imposed if any person knowingly:

   (a) uses or causes to be used a unique health identifier;
   (b) obtains individually identifiable health information relating to an individual; or
   (c) discloses individually identifiable health information to another person, obtains or discloses individually identifiable health information in violation of HIPAA requirements.

42 U.S.C. § 1320d-6(a)

2. Penalties are as follows for persons who knowingly violate HIPAA requirements:

(a) Fine of not more than $50,000, imprisoned not more than 1 year, or both;
(b) If the offense is committed under false pretenses, a fine of not more than $100,000, imprisoned not more than 5 years, or both; and
(c) If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000, imprisoned not more than 10 years, or both.

42 U.S.C. § 1320d-6(b)

C. Civil Penalties

The ARRA has strengthened the civil sanctions which apply to violations of HIPAA. ARRA § 13410. There are provisions for individuals to receive a portion of penalties received by HHS after the GAO conducts and study and HHS adopts rules for such distributions. ARRA § 13410(c).

The following table shows categories of violations and respective penalty amounts available as set forth in § 160.404:

Violation category—Section 1176(a)(1)	**Each violation**	**All such violations of an identical provision in a calendar year**
(A) Did Not Know.....	$100–$50,000	$1,500,000
(B) Reasonable Cause.....	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected..	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

Reasonable cause means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

For violations occurring on or after February 18, 2009, the following affirmative defenses are available under §160.410:

1. The violation is subject to criminal penalties, or

2. The covered entity establishes that the violation is:

   (a) Not due to willful neglect and
   (b) Corrected during either:

      (i) The 30 day period on which the covered entity knew or reasonably should have known, that the violation occurred; or
      (ii) Such additional time as the Secretary of HHS determines to be appropriate.

The Secretary has authority to waive imposition of civil penalties if a penalty would be excessive relative to the violation. §160.412.

XXII. Enforcement

There is no private right of action. 65 Fed. Reg. 82566 (12/28/2000).

Enforcement may be through the HHS Office of Civil Rights. 65 Fed. Reg. 82472 (12/28/2000) or through the State Attorney General.

The scope of relief available through an Attorney General is substantially lower than what is available from HHS: $100 per violation with a maximum of $25,000 per year for identical violations.