

Law Office of David L. McGuffey, LLC
202 W. Crawford Street, Suite B
Dalton, Georgia 30720
(706) 428-0888
www.primetimelaw.com

**HIPAA Revisited: Speaking Notes for 3/25/04 ATLA
Teleconference¹**

As recently as last week [March 2004], one commentator wrote that “a national consensus about planning responses to HIPAA has not yet emerged.”

So, ... what is HIPAA?

1. Purpose of HIPAA.

“HIPAA” is shorthand for the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The text of the law ([42 U.S.C. ' 1320d through 1320d-8](#) is an appendix to this paper).

While HIPAA covers a number of subjects, the primary focus here is on the privacy rules relating to health information.

The privacy rules are primarily found in regulations promulgated by the Department of Health and Human Services.

The regulations indicate that there are **three purposes**: “(1) *To protect and enhance the rights of consumers by providing them access to their health information* and controlling the inappropriate use of that information; (2) to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals and the multitude of organizations and individuals committed to the delivery of health care; and (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.” 65 FR 82462, Standards for Privacy of Individually Identifiable Health Information, December 28, 2000 (emphasis added).

HIPAA is a shield. It is not a sword that can be used to prevent the patient from gaining access to his or her own records.² HIPAA’s purpose is to ensure individual

¹ Portions of this paper were originally presented in a previous ATLA Teleconference regarding HIPAA.

² One of the stated purposes of HIPAA is “Ensuring patient access to their medical records. Patients must be able to see and get copies of their records, and request amendments. In addition, a history of most disclosures must be made accessible to patients.” See HHS Fact Sheet, <http://aspe.hhs.gov/admsimp/final/pvcfact1.htm>.

privacy and autonomy concerning the use of health information. The regulations refer to Justice Brandeis' words in stating "If the right to be left alone means anything, then it likely applies to having outsiders have access to one's intimate thoughts, words, and emotions." 65 FR, at 82464.

There is no private right of action under HIPAA. Anyone reviewing claims under HIPAA would be advised to review **Cort v. Ash, 422 U.S. 66 (1975)**. There, the Supreme Court created a four part test for determining whether an implied right of action exists. **The test is:** (1) whether the statutes were created for the plaintiffs' special benefit, (2) whether there is evidence of legislative intent to create a private remedy, (3) whether a private remedy would be consistent with legislative purposes, and (4) whether the area is one traditionally relegated to the states. In the context of OBRA (nursing home resident rights), Courts have generally declined to find that a private right of action exists because health care is a subject traditionally relegated to the states. See, e.g., Brogdon v. NHC, 103 F.Supp2d 1322 (N.D. Ga. 2000).

2. History.

The Health Insurance Portability and Accountability Act (HIPAA) was signed by the President and became law on August 21, 1996 (P.L. No. 104-191). HIPAA's legislative history is found on the internet at <http://thomas.loc.gov>.

The "privacy" provisions of HIPAA comprise a small portion of the Act and are found at Title II, subtitle F, sections 261-264. They are codified at 42 U.S.C. § 1320d through § 1320d-8.

Congress directed HHS to make recommendations regarding how best to protect private health data and, assuming it failed to act on those recommendations, directed HHS to develop regulations. Specifically, **Section 264 of HIPAA provides** that:

"(a) Not later than 12 months after the date of enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information. (b) **The recommendations under subsection (a) shall address at least the following:**

- (1) The rights that an individual who is a subject of individually identifiable health information should have.**
- (2) The procedures that should be established for exercise of such rights.**
- (3) The uses and disclosures of such information that should be authorized or required.**

(c) (1) **If legislation governing standards with respect to the privacy of individually identifiable health information** transmitted in connection with the

transactions described in section 1173(a) of the Social Security Act (as added by section 262) **is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations** containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b). (c)(2) A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications under the regulation. (d) In carrying out this section, the Secretary of Health and Human Services shall consult with (1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and (2) the Attorney General.” (Emphasis added).

In September, 1997, HHS delivered recommendations to Congress for protecting the privacy of individually identifiable health information. See South Carolina Medical Association v. Thompson, 327 F.3d 346, 349 (4th Cir. 2003). Congress did not pass any additional legislation. Id.; 65 FR, at 82470. Thus, under HIPAA’s mandate, HHS drafted regulations that appeared in a November 3, 1999 Notice of Proposed Rulemaking (See 64 FR 59918). South Carolina Medical Ass’n, supra.

The proposed rule drew more than 50,000 comments from affected parties. Id. After several further proposals, HHS promulgated final regulations in February 2001. Id. Those rules appear at [45 C.F.R. § 164.500 through § 164.534](#).

The HIPAA regulations were recently challenged as an unconstitutional delegation of congressional power, as going beyond HIPAA’s authority, in that HIPAA relates primarily to electronic data transmission, while the regulations apply to all health records regardless of form, and as vague. These challenges were rejected. See South Carolina Medical Ass’n, supra.

3. Other laws.

State laws more stringent than HIPAA remain in effect. Regulations define what “more stringent” means as follows: “in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria: (1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is: (i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or (ii) To the individual who is the subject of the individually identifiable health information.” 45 C.F.R. § 160.202.

Summaries of various state laws relating to health privacy can be downloaded at <http://www.healthprivacy.org>. Because we practice in Georgia and Tennessee, focusing on long term care issues, we briefly review those rules.

A. Georgia.

O.C.G.A. § 31-33-2(a)(2) provides “Upon written request from the patient or a person authorized to have access to the patient’s record under a health care power of attorney for such patient, the provider having custody and control of the patient’s record shall furnish a complete and current copy of that record, in accordance with the provisions of this Code section. If the patient is deceased, such request may be made by a person authorized immediately prior to the decedent’s death to have access to the patient’s record under a health care power of attorney for such patient; the executor, temporary executor, administrator, or temporary administrator for the decedent’s estate; or any survivor, as defined by Code Sections 51-4-2, 51-4-4, and 51-4-5.” The provider may refuse a request to deliver records to the patient if the provider reasonably determines that disclosure of the record to the patient will be detrimental to the physical or mental health of the patient. O.C.G.A. § 31-33-2(c). However, in that instance, the patient’s record shall, upon written request by the patient, be furnished to any other provider designated by the patient. *Id.* A provider may refuse to disclose records until a proper authorization is received with evidence of authority to sign said release. O.C.G.A. § 31-33-2(d). A fee may be charged for records. O.C.G.A. § 31-33-3.

Residents in long term care facilities have a right to access all medical records relating to their treatment. O.C.G.A. § 31-8-108(b)(6) provides: “Each resident shall have access to all information in the medical records of the resident and shall be permitted to inspect and receive a copy of such records unless medically contraindicated. The facility may charge a reasonable fee for duplication, which fee shall not exceed actual cost.”

B. Tennessee.

T.C.A. § 63-2-101(a)(1) provides: “Notwithstanding any other provision of law to the contrary, a health care provider shall furnish to a patient or a patient's authorized representative a copy or summary of such patient's medical records, at the option of the health care provider, within ten (10) working days upon request in writing by the patient or such representative.” T.C.A. § 63-2-101(c)(2) defines “Medical records” as “all medical histories, records, reports and summaries, diagnoses, prognoses, records of treatment and medication ordered and given, x-ray and radiology interpretations, physical therapy charts and notes, and lab reports.” Medical records are subject to subpoena from a court of competent jurisdiction. T.C.A. § 63-2-101(b)(1) and (d). Section 63-2-102 provides for fees that may be charged.

Hospital records are governed by T.C.A. §§ 68-11-301 to 68-11-311. Section 68-11-304(a)(1) provides: “Unless restricted by state or federal law or regulation, a hospital shall furnish to a patient or a patient's authorized representative such part or parts of such patient's hospital records without unreasonable delay upon request in writing by the patient or such representative.” The phrase “Hospital records” means “those medical histories, records, reports, summaries, diagnoses, prognoses, records of treatment and medication ordered and given, entries, X-rays, radiology interpretations, and other written, electronic, or graphic data prepared, kept, made or maintained in hospitals that

pertain to hospital confinements or hospital services rendered to patients admitted to hospitals or receiving emergency room or outpatient care.” T.C.A. § 68-11-302(5)(A). Section 304 provides for a fee reference furnishing records.

Prior to the execution of a nursing home admissions contract, disclosure must be provided that references the resident’s right to review medical records. T.C.A. § 68-11-910(a)(3).

C. OBRA (Nursing Home Residents).

HIPAA does not alter a nursing home resident’s right to access medical records.

The preamble to the final rule (December 2000 – 65 FR 82480) states: “Covered entities subject to these rules are also subject to other federal statutes and regulations.” “If a statute or regulation prohibits dissemination of protected health information, but the privacy regulation requires that an individual have access to that information, the earlier, more specific statute would apply. ... From our review of several federal laws, it appears that Congress did not intend for the privacy regulation to overrule existing statutory requirements in these instances.” 65 FR 82482.

See 42 U.S.C. § 1395i-3(c)(1)(A)(iv) (facilities that accept Medicare residents); 42 U.S.C. § 1396r(c)(a)(A)(iv) (facilities that accept Medicaid residents); 42 C.F.R. § 483.10(b)(2) (all facilities that accept Medicare and/or Medicaid residents). Specifically, 42 C.F.R. § 483.10(b)(2) provides: The resident or his or her legal representative has the right (i) Upon an oral or written request, to access all records pertaining to himself or herself including current clinical records within 24 hours (excluding weekends and holidays); and (ii) After receipt of his or her records for inspection, to purchase at a cost not to exceed the community standard photocopies of the records or any portions of them upon request and 2 working days advance notice to the facility.

OBRA	HIPAA
All records pertaining to the resident may be accessed	Designated record set may be accessed; authorizes exceptions, such as psychotherapy notes.
Records must be produced within 24 hours (excluding weekends and holidays) and copies must be provided within 2 business days	Records that are on-site must be produced within 30 days, with one 30 extension permitted; records that are off-site must be produced within 60 days, with one 30 day extension permitted
Absolute right	Request may be denied under certain circumstances
42 CFR 483.10(b)(2)	45 CFR 164.524(b)

Analysis where there is conflicting federal law. (1) Is the disclosure required by other federal law. If the answer is “Yes”, then it is permissible to disclose records. [45 CFR 164.512\(a\)](#).³

The U.S. Department of Health and Human Services has posted a compilation of “questions and answers” on its website. Among them is the following:

Question: Does the HIPAA Privacy Rule permit nursing homes and other health care institutions to disclose information concerning admissions of supplemental security income (SSI) recipients to the Social Security Administration (SSA)?

Answer: Yes. SSA requires nursing homes, extended care facilities, and intermediate care facilities to report to SSA, within 2 weeks, admissions information about anyone receiving SSI who is admitted to the institution. The purpose of these reporting requirements is to prevent SSI overpayments caused by a SSI recipient’s failure to timely report changes in eligibility. These requirements are stated in the Social Security Act (42 U.S.C. 1383(e)(1)(C)), and communicated through SSA’s guidance and other implementation materials. The Privacy Rule permits covered entities to disclose protected health information without the individual’s authorization as required to comply with this law. See [45 CFR 164.512\(a\)](#).

This analysis suggests that OBRA regulations requiring disclosure to residents would likewise apply.

4. Application:

The HIPAA rules focus, in part, on encouraging “a more informed interaction between the patient and the [health care] provider during the consent process.” 65 FR, at 82473. Under the regulations, a consent form must be accompanied by a notice describing the health care provider’s privacy policy and the consent form must reference that privacy policy. The following summary provides an overview of HIPAA’s application:

- A. **When is HIPAA Effective?** Most provisions of HIPAA are effective as of April 14, 2003. There are certain exceptions to this rule for small providers. Small health plans, defined as plans with annual receipts of less than \$5 million, must comply no later than April 14, 2004.
- B. **Who Does HIPAA apply to?** HIPAA applies to all “covered entities” which generally include all “health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction. [42 C.F.R. § 164.104](#). In the current

³ Required by law is limited to disclosures that are enforceable in a court of law. [45 CFR 164.501](#). However, a non-exclusive list of examples of what “required by law” means are provided and, among them, is the following: Medicare conditions of participation with respect to health care providers participating in the program. The same analysis should apply to providers participating in the Medicaid program. Thus, even if there is no private right of action under HIPAA, OBRA should still apply and records may be secured in most nursing home litigation contexts. In addition, state laws which create a private right of action, such as the Georgia Bill of Rights for Residents of Long Term Care Facilities, would fit that requirement.

market, virtually all health care providers will transmit some data in electronic form, either to recover payment under Medicare, Medicaid, or from an insurance carrier. Thus, given the breadth of the regulations, HIPAA will apply to virtually all health care providers.

There is a decision tree for determining whether an entity is a “covered entity” at the CMS website. Go to www.cms.gov and click on the HIPAA link on the left hand side of the page. Then to Decision Tools.

- C. **Who are Health Care Providers?** The phrase “Health care provider” is defined as “a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.” 45 C.F.R. § 160.103. “Health care” means “care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) preventative, diagnostic, therapeutic, rehabilitation, maintenance, or palliative care, and counseling; service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. *Id.*”
- D. **What type of information is covered?** According to a fact sheet produced by the U.S. Department of Health and Human Services, “**All medical records and other individually identifiable health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally, is covered by the final regulation.**” See [HHS Fact Sheet, http://aspe.hhs.gov/admnsimp/final/pvcfact1.htm](http://aspe.hhs.gov/admnsimp/final/pvcfact1.htm). The regulations define “Health information” as “any information , whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.” 45 C.F.R. § 160.103. Health information is “**Protected health information**” if it is “individually identifiable health information and is (i) transmitted by electronic media; (ii) maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or (iii) **transmitted or maintained in any other form or medium.**” 45 C.F.R. § 164.501 (emphasis added). Certain exclusions related to education and employment records are found at [45 C.F.R. § 164.501](#). “Individually identifiable health information” is “information that is a subset of health information, including demographic information

collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 164.501. HIPAA further defines a “**Designated record set**” as “(1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.” 45 C.F.R. § 164.501.

Practice Note: Consider drafting discovery requests to incorporate HIPAA’s terminology. For example, in addition to requesting specific documents you are seeking, request “protected health information as that term is defined in 45 C.F.R. § 164.501” or request the “Designated record set as that phrase is defined in 45 C.F.R. § 164.501”

- E. **What type of activity is covered?** “A covered entity may not use or disclose protected health information, except as permitted or required by [HIPAA]. 45 C.F.R. § 164.502. “Disclosure” means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.” 45 C.F.R. § 164.501. “Use” means “with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.” 45 C.F.R. § 164.501.
- F. **Minimum necessary standard.** HIPAA imposes a “minimum necessary standard” on health care providers when using or disclosing protected health information. 45 C.F.R. § 164.502(b)(1). A covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. *Id.*

Practice Note: The “minimum necessary” standard does not apply to disclosures to the patient or pursuant to a valid authorization. 45 C.F.R. § 164.502(b)(2)(ii) and (iii). Nonetheless, when drafting medical releases, draw them broadly enough to capture all information that will be necessary to present your case. Otherwise, the health

care provider may withhold certain information in an attempt to comply with the “minimum necessary” standard.

5. Internal Use of Information.

Prior to August 14, 2002, health care providers were required to secure “consent” from patients prior to any use of health care information. HHS received numerous comments describing situations where direct treatment would be inhibited by that rule. Now, health care providers are not required to secure patient consent prior to using health information for its own treatment, payment and health care operations. See 67 FR, at 53209. HIPAA expressly states that a covered entity may use or disclose protected health information for treatment, payment, or health care operations. 45 C.F.R. § 164.502(a)(1)(ii) and § 506(a) and (c).

Practice note: Since HIPAA authorizes internal use and disclosure of protected health information, it does not alter the standard of care regarding how a facility uses (or should use) information within its control.

Except as otherwise permitted or required under HIPAA, a covered entity may not use or disclose protected health information without an authorization that complies with 45 C.F.R. § 164.508(a)(1).

With respect to psychotherapy notes, an authorization is required if those notes are to be used by or disclosed to any person other than the originator of the notes in connection with treatment, except where used in connection with internal training programs or in defending itself in an action brought by the patient. 45 C.F.R. § 164.508(a)(2).

6. Who May Request Information?

HIPAA was not designed to prevent patients from accessing their own data. Thus, a covered entity may always provide access to protected health information to the patient, or pursuant to a valid authorization. 45 C.F.R. § 164.502(a)(1)(i) and (a)(1)(iv). Further, the regulations expressly provide that a patient has a right of access to inspect and copy information in a designated record set except for certain information. 45 C.F.R. § 164.524(a)(1) and (b)(1). The exceptions apply to psychotherapy notes; information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, and certain protected information subject to the Clinical Laboratory Improvements Amendments of 1988. 45 C.F.R. § 164.524(a)(1). Consult state law as well regarding a patient’s right of access.

When access to records is requested, the covered entity must act on the request within 30 days. 45 C.F.R. § 164.524(b)(2). Where the request is for records not maintained on-site, the covered entity may have up to 60 days to respond. Section

524(b)(2)(ii). If the covered entity is unable to comply within the timeframe requested, it may have one 30 day extension. 524(b)(2)(iii). Regardless of whether access is granted or denied, the covered entity must inform the patient of its intent. Section 524(b)(2)(i)(A) and (B).

7. Personal Representatives.

HIPAA does not alter any laws relating to an agent's right to access health care information. Specifically, with few exceptions, a covered entity must treat a personal representative as the patient for purposes of the regulations. 45 C.F.R. § 164.502(g)(1). "If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under [HIPAA] with respect to protected health information relevant to such personal representation." 45 C.F.R. § 164.502(g)(2) (emphasis added). HHS received comments regarding a prior version of the rule which used the phrase "power of attorney" and, on review, deleted the phrase. The rule was clarified so that "the rights and authorities of a personal representative under this rule are limited to protected health information relevant to the rights of the person to make decisions about an individual under other law. For example, if a husband has authority only to make health care decisions about his wife in an emergency, he would have the right to access protected health information related to that emergency, but he may not have the right to access information about treatment that she had ten years ago." 65 FR, at 82634.

Practice Note: When drafting powers of attorney, be certain to fully comply with all requirements relating to health care powers of attorney and draft them broadly enough to encompass all related time periods and health care procedures.

One of the "question and Answer" sets on the DHHS website addresses whether a personal representative acting under a non-health care POA may request medical records. The answer from DHHS was "no."

Informal decision makers, such as a family member or the responsible person for a nursing home resident may have access to protected health information "relevant to such person's involvement with the individual's care or payment related to the individual's health care." 45 C.F.R. § 164.510(b)(1)(i). If the patient is present, the health care provider must do one of the following: (1) obtain the patient's consent; (2) provide the patient with the opportunity to object and determine that there was no objection; or (3) reasonably infer that the individual does not object to the disclosure. If the patient is not present, or if incapacitated, then the health care provider may disclose protected health information is, in the exercise of professional judgment, it is determined to be in the patient's best interests. The regulations specifically state that professional judgment may be used in allowing a family

member to pick up filled prescriptions, medical supplies, etc. See also 65 FR, at 82634.

Similarly, persons authorized to act for the estate of a deceased individual must be treated as the individual. [45 C.F.R. § 164.502\(g\)\(4\)](#). However, the rule is broader for personal representatives of estates than it is for representatives of living person. “A person may be a personal representative of a deceased individual if they have the authority to act on behalf of such individual or such individual’s estate for any decision, not only decisions related to health care. We create a broader scope for a person who is a personal representative of a deceased individual because the deceased individual can not request that information be disclosed pursuant to an authorization, whereas a living individual can do so.” 65 FR, at 82634.

Where the covered entity has a reasonable belief that abuse will occur, it may elect not to treat the personal representative as the individual. [45 C.F.R. § 164.502\(g\)\(5\)](#).

“The determination about who is a personal representative under [HIPAA] is based on state or other applicable law.” 65 FR, at 82634. The only requirement HIPAA adds is verification of the agent’s authority. Id; [45 C.F.R. § 164.514\(h\)](#). In that regard, the health care provider must obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under [section 514\(h\)](#).

The health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information by alternative means or at alternative locations. [45 C.F.R. § 164.522\(b\)\(1\)](#).

Practice Note: Section 164.522(b)(1) would authorize persons such as the personal representative of a nursing home resident, or attorney, to designate another location as the delivery point for protected health information.

8. Authorizations; Proper Form.

The HIPAA federal regulations provide: “If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under [HIPAA] with respect to protected health information relative to such personal representation.” [45 C.F.R. ' 164.502\(g\)\(2\)](#).

A medical records release is invalid under HIPAA unless it complies with [45 C.F.R. § 164.508\(b\) and \(c\)](#). Except in limited circumstances, an authorization cannot be combined with another document. [45 C.F.R. § 164.508\(c\)\(3\)](#). An authorization can be

revoked at any time except, to the extent that a covered entity has taken action in reliance on the authorization or in certain disputes over coverage where a policy of insurance was issued. [45 C.F.R. § 164.508\(c\)\(5\)](#).

Briefly, the regulations provide that a release must include the following “core elements”:

- (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- (ii) The name or other specific identification of the person or class of person authorized to make the requested use of disclosure;
- (iii) The name or other specific identification of the person or class of person to whom the covered entity may make the requested use or disclosure;
- (iv) A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;
- (v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including the creation and maintenance of a research database or research repository;
- (vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such person’s authority to act for the individual must also be provided;
- (vii) A statement of the individual’s right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
- (viii) A statement that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by this rule;
- (ix) Other elements apply where the requesting party is, itself, a covered entity. Those elements are not covered herein.

See [45 C.F.R. § 164.508\(c\)](#).

An authorization must be written in plain English. [45 C.F.R. § 164.508\(c\)\(3\)](#). A form of release is attached at the end of these materials.

9. Authorization Not Required.

The HIPAA regulations outline a number of instances where no authorization is required to secure health information. Those regulations appear at [45 C.F.R. § 160.510 and 512](#).

A. **Emergency Situations.** No authorization is required in cases of incapacity or emergency where the health care provider is acting consistent with a prior expressed preference and in the patient's best interests. [45 C.F.R. § 164.510\(a\)\(3\)](#).

B. **Family and Friends.** Protected health information may be disclosed to family and friends provided: (i) if the patient is present and may object, an opportunity to object to the disclosure is provided and none is expressed; or (ii) if the patient is unable to express an objection, the covered entity determines that disclosure is in the patient's best interests and disclosure is limited to information directly relevant to the third party's involvement with the patient's health care. [45 C.F.R. § 164.510\(b\)](#).

C. **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 law. [45 C.F.R. § 164.512\(a\)\(1\)](#). "Required by law" means a mandate contained in law that compels an entity to make use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require production of information; a civil or authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits." [45 C.F.R. § 164.501](#). Disclosures which are "required by law" must be consistent with requirements in the following:

(i) **Disclosures about victims of abuse, neglect or domestic violence.** [45 C.F.R. § 164.512\(c\)](#). These are primarily disclosures to government agencies and are not discussed herein.

(ii) **Disclosures for judicial and administrative proceedings.** [45 C.F.R. § 164.512\(e\)](#). A covered entity may

disclose protected health information in the course of any judicial or administrative proceeding: (i) in response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or (ii) in response to a subpoena, discovery request, or other lawful process, that is not accompanied by a court order of a court or administrative tribunal, if: (A) the covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii)⁴ of this section, from the party seeking the information, that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or (B) the covered entity receives satisfactory assurances, as described in paragraph (e)(1)(iv)⁵ of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v)⁶ of this section. A covered entity may, nonetheless disclose protected health information in response to lawful process without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (b) if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv).

⁴ Section (e)(1)(iii) provides that a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrative that: (A) the party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); (B) the notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and (C) the time for the individual to raise objections to the court or administrative tribunal has elapsed, and (1) no objections were filed; or (2) all objections filed by the individual have been resolved by the court or administrative tribunal and the disclosures being sought are consistent with such resolution.

⁵ Section (e)(1)(iv) provides that a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that: (A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or (B) the party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

⁶ Section (e)(1)(v) provides that a qualified protective order means, with respect to protected health information requested under section (e)(1)(ii), an order from a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (A) prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and (B) requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding. A form qualified protective order is included at the end of these materials.

Practice Note: Since an individual may always request his or her own records, consider whether this exception would authorize access to a third party's protected health information where such information is relevant to the litigation.

See also Sources at §§ 9.1 through 9.3 in Hare et al Full Disclosure: Combating Stonewalling and Other Discovery Abuses (ATLA Press 1995).

(iii) Disclosures for law enforcement purposes. 45 C.F.R. § 164.512(f). These disclosures are not discussed herein.

- D. **Public health activities.** Disclosure to public health authorities is authorized, but is not discussed here. 45 C.F.R. § 164.512(b)(1).
- E. **Disclosures about decedents.** Covered entities may make appropriate disclosure to coroners, medical examiners and funeral directors. 45 C.F.R. § 164.512(g).
- F. **Tissue donation.** Covered entities may make appropriate disclosures regarding tissue and organ donations. 45 C.F.R. § 164.512(h).
- G. **Research.** Covered entities may make appropriate disclosures for research purposes where certain privacy programs are in place. 45 C.F.R. § 164.512(i).
- H. **Disclosures to avert a serious threat to health or safety.** Where a covered entity, in good faith, believes that use or disclosure of protected health information is necessary to prevent a threat to health or safety, certain disclosure is permitted. 45 C.F.R. § 164.512(j).
- I. **Specialized government functions.** Certain disclosures are authorized in connection with specialized government functions (e.g., military and veterans activities). 45 C.F.R. § 164.512(k).
- J. **Workers compensation.** Covered entities may make disclosures necessary to comply with worker's compensation laws. 45 C.F.R. § 164.512(l).

Standing Orders: I am aware of at least one worker's compensation judge who has issued a standing qualified protective order. You might consider whether this would facilitate discovery in courts where you practice regularly and approach the senior judge about entering such an order.

In addition, information that does not identify an individual, or where there is a “very small” risk that the individual may be identified may be disclosed under certain circumstances. [45 C.F.R. § 164.514](#). A substantial amount of data must be redacted to comply with this rule.

10. Summary of Methods That May be Used to Secure Records.

The patient (or Nursing Home resident) always has a right to access his or her own records. No “release” is required for personal access. Questions arise when surrogate decision makers or third-parties (e.g. lawyers) seek to access records.

1. HIPAA Release (necessary where there is no decision-making power);
2. Health Care Power of Attorney (decision making power);
3. Guardianship/Conservatorship (decision making power);
4. Statute authorizing Health Care decisions (often limited to emergencies);
5. Qualified Protective Order.
6. Emergencies: Disclosure is permitted in two circumstances:
 - a. when the patient has “capacity to make health care decisions” and verbally consents, is present or otherwise available, or the provider reasonably infers, “based on the exercise of professional judgement,” that consent is being given. [45 CFR 164.510\(b\)\(2\)](#); and
 - b. When the patient is not present, or not able to give consent because of incapacity or an emergency circumstance. [45 CFR 164.510\(b\)\(3\)](#)

11. Notices.

Under [section 164.520](#), an individual has a right to adequate notice of the uses and disclosures of protected health information and of the individual’s rights and the covered entities legal duties with respect to protected health information. The notice must address the individual’s right to inspect and copy protected health information. [45 C.F.R. § 164.520\(b\)\(1\)\(iv\)\(C\)](#). The notice must also contain a statement that the covered entity is required to abide by the terms of its current notice, and must describe how any change in the notice would become effective.

Practice Note: Any refusal to provide information should be compared to the covered entity’s notice and, if it is inconsistent with that notice, the refusal is inappropriate.

12. Whistleblowers.

HIPAA makes specific provision for whistleblowers. The provision, while narrow, would allow a nursing home employee, for example, to disclose information to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee relevant conduct, or to an appropriate health care accreditation organization, where the employee believes in good faith that conduct is unlawful,

that it violates professional or clinical standards, or that care or services endangers one or more patients, workers of the public. [45 C.F.R. § 164.502\(j\)](#).

13. Law Firms.

An article in the June, 2003, issue of Health Lawyers News (page 8), makes the argument that a law firm may be a HIPAA business associate. This would be true if the covered entity provides the law firm with any protected health information and demographic information (such as a list of patients) is sufficient. If so, regulations applicable to business associates will apply to law firms (primarily defense firms). For example, a business associate is subject to HIPAA rules that give a patient the right to amend protected health information. (To be discussed by I. Ellerin). Consider how that might impact the trial of your case.

14. Recent Cases.

NATIONAL ABORTION FEDERATION, et al., Plaintiff, v. John ASHCROFT, Defendant. NORTHWESTERN MEMORIAL HOSPITAL, Movant., 2004 WL 292079 (N.D.Ill.)

Litigation challenged constitutionality of the Partial Birth Abortion Ban Act of 2003. As part of the litigation, the government served Northwestern with a subpoena pursuant to Federal Rule of Civil Procedure 45. The subpoena sought production of "[a]ll medical records associated with those medical record numbers to be identified by [Dr. Hammond] in response to the discovery demand served upon him" in *NAF*. Accompanying the subpoena was an Order signed by District Judge Richard Conway Casey, who is presiding over the litigation in New York. The Order authorizes Northwestern, as a non-party witness, to disclose to the government the medical records sought by the attached subpoena in accordance with the **Health Insurance Portability and Accountability Act of 1996 ("HIPAA")**, Pub.L. No. 104-191, §§ 261-264, 110 Stat.1936 (Aug. 21, 1996), and 45 C.F.R. § 64.512(e)(1)(i).

There was an agreement that identifying information would be redacted. Still, Northwestern moved to quash the subpoena as violating both HIPAA and State privacy laws. With respect to HIPAA, the Court found:

"In other words, **HIPAA's** regulations clearly allow a hospital to disclose patient medical records, when ordered in judicial proceedings, subject to the above limitations."

However, under Illinois law, courts have reasoned that even if a patient's name and identification number are redacted from his or her file, because prior and present medical history would still be disclosed, the patient's right to confidentiality could potentially be compromised.

Important for several reasons.

1. The decision defines a conflict between HIPAA and State law as a situation where a "covered entity would find it impossible to comply with both the State and federal requirements." 45 C.F.R. § 160.202. HIPAA overrules the State law where the State law provides less privacy. However, where the State law provides more protection, the State law is followed.
2. **HIPAA** and the regulations promulgated thereunder, not Federal Rule of Evidence 501, control the protections provided to patient medical records held by hospitals.

3. Because **HIPAA**, not Federal Rule of Evidence 501, governs how individually identifiable health information, such as medical records, should be kept private, Illinois law controls and the government's subpoena must be quashed.
4. This case tells us something about how third party records may be accessed. The Court makes it clear that nothing in HIPAA prohibits disclosure under a qualified protective Order in the absence of a more restrictive State law. If the parties were able to satisfy Illinois State law privacy requirements, then the records could be disclosed.
5. Finally, this is an example of a situation where discovery was shut down through the use of health care privacy laws.
6. Other notes:
 - i. the court recognized a physician-patient privilege under Fed. Rule Ev. 501, at least in the context of an abortion.
 - ii. The utility of the information sought was questionable. The government sought it on the possibility that relevant information could be gain.

Solomon v. State Board, 2003 WL 22976547 (Md. App.)

HIPAA does not prevent disclosure of records to a licensing or disciplinary agency.

A HELPING HAND, LLC v. BALTIMORE COUNTY, MARYLAND, et al., 295 F.Supp.2d 585

“Even assuming the patient data is covered by **HIPAA**, the **HIPAA** regulations permit discovery of protected health information so long as a court order or agreement of the parties prohibits disclosure of the information outside the litigation and requires the return of the information once the proceedings are concluded. *See* 45 C.F.R. § 164.512(e). While no such order or agreement is yet in effect, the parties presumably could obtain one. As for the cited Maryland provisions, the privileges they establish are not applicable here because this lawsuit is governed by federal, rather than state, law. *See* Fed.R.Evid. 501.”

Joseph FAVOR, Plaintiff, v. Cibel HORNE, Defendant. 767 N.Y.S.2d 205

In personal injury action, subpoena issued to secure medical records must comply with HIPAA and with State law.

David HUTTON, Plaintiff, v. CITY OF MARTINEZ, et al., Defendants., 219 F.R.D. 164

No physician-patient privilege in Federal Court. “The Court finds that **HIPAA** does not preclude production of the medical records and worker's compensation files in response to either a discovery request, subpoena or this Court's order, under an adequate protective order. There is already a protective order in this case, which adequately safeguards the defendant's privacy.”

In re: PPA LITIGATION, 2003 WL 22203734 (N.J.Super.L.)

Concerned ex parte communication with health care providers by Defense council. The practice was not precluded, but could not be conducted without compliance with HIPAA. “[O]ur task is deciding the narrow issue of whether **HIPAA** preempts the informal discovery techniques. The answer is plainly no.” However, the authorization in use did not provide sufficient safeguards to protect privacy, so a new authorization was required which complies with HIPAA.

Other resources: www.LawyersandHIPAA.com, <http://www.lawyersandhipaa.com/Resources.htm>.

Conclusion

Traditional methods of securing medical records are no longer adequate. HIPAA continues to evolve. It is no longer a mystery, but it must be considered when medical records must be secured. A failure to make oneself knowledgeable concerning HIPAA's rules will result in delays securing records and, in certain cases, may result in the Plaintiff or patient advocate failing to secure records. The result, in such a case, might be a failure to secure information necessary to prove an injury and/or to show that care received to-date is substandard. Thus, it is incumbent on us, as the Advocate, to learn HIPAA's rules so we can navigate this new regulatory environment.

Appendix: Form of Release/Authorization

**VALID AUTHORIZATION UNDER 45 CFR Sec. 164.508
(HIPAA AUTHORIZATION)**

Pursuant to 45 CFR Sec. 164.502(a)(1)(iv) a covered entity is permitted to disclose protected health information pursuant to and in compliance with a valid authorization under Sec. 164.508.

I, _____, an individual, hereby authorize:

1. Any and all health care providers and/or other persons or entities who have possession of any protected health information relating to me,
2. to disclose any and all protected health information, including, but not limited to any and all designated record sets, medical records of every form or description, billing records of every form or description,
3. to: David L. McGuffey and his employees, at:

Law Office of David L McGuffey, LLC 202 W. Crawford Street, Suite B Dalton, GA 30720 (706) 428-0888
--

4. The persons in paragraph 3 of this Release are authorized to request any and all protected health information covered by this Release, or may specify particular information. The purpose of this Release is at my request and for my convenience. The protected health information requested shall be timely delivered to the persons and to one of the addresses in paragraph 3 or by any other delivery method they request in writing.
5. I understand that I am not required to execute this release, that I may refuse to do so, and that no treatment or benefits eligibility is conditioned on its execution. I understand that I may revoke this release by delivering written notice to my Attorneys, but I agree I will not do so while they are representing me. This authorization shall terminate on the first to occur of: (1) my death or (2) upon my written revocation actually received by the covered entity. Proof of receipt of my written revocation may be by certified mail, registered mail, facsimile, or any other receipt evidencing actual receipt by the covered entity. This revocation shall be effective upon the actual receipt of the notice by the covered entity except to the extent that the covered entity has taken action in reliance on it. By signing this Authorization, I acknowledge that the information used or disclosed pursuant to this authorization may be subject to redisclosure by the person or persons whose name is written in paragraph 3 of this authorization and the information once disclosed will no longer be protected.

Signed this ____ day of _____, 2004.

Patient

WITNESS

NOTARY

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE
CHAPTER 7 - SOCIAL SECURITY
SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE
SIMPLIFICATION
Part C - Administrative Simplification

-HEAD-

Sec. 1320d. Definitions

-STATUTE-

For purposes of this part:

(1) Code set

The term 'code set' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

(2) Health care clearinghouse

The term 'health care clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

(3) Health care provider

The term 'health care provider' includes a provider of services (as defined in section 1395x(u) of this title), a provider of medical or other health services (as defined in section 1395x(s) of this title), and any other person furnishing health care services or supplies.

(4) Health information

The term 'health information' means any information, whether oral or recorded in any form or medium, that -

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

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

(5) Health plan

The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 300gg-91 of this title). Such term includes the following, and any combination thereof:

(A) A group health plan (as defined in section 300gg-91(a) of this title), but only if the plan -

(i) has 50 or more participants (as defined in section 1002(7) of title 29); or

(ii) is administered by an entity other than the employer who established and maintains the plan.

(B) A health insurance issuer (as defined in section 300gg-91(b) of this title).

(C) A health maintenance organization (as defined in section 300gg-91(b) of this title).

(D) Parts (FOOTNOTE 1) A, B, or C of the Medicare program under subchapter XVIII of this chapter.

(FOOTNOTE 1) So in original. Probably should be 'Part'.

(E) The medicaid program under subchapter XIX of this chapter.

(F) A Medicare supplemental policy (as defined in section 1395ss(g)(1) of this title).

(G) A long-term care policy, including a nursing home fixed indemnity policy (unless the Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).

(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.

(I) The health care program for active military personnel under title 10.

(J) The veterans health care program under chapter 17 of title 38.

(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of title 10.

(L) The Indian health service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.).

(M) The Federal Employees Health Benefit Plan under chapter 89 of title 5.

(6) Individually identifiable health information

The term "individually identifiable health information" means any information, including demographic information collected from an individual, that -

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

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

-

(i) identifies the individual; or

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

(7) Standard

The term "standard", when used with reference to a data element of health information or a transaction referred to in section 1320d-2(a)(1) of this title, means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1320d-1 through 1320d-3 of this title.

(8) Standard setting organization

The term "standard setting organization" means a standard setting organization accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation of this part.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1171, as added Pub. L.

104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2021;
amended Pub. L. 107-105, Sec. 4, Dec. 27, 2001, 115 Stat. 1007.)

-REFTEXT-

REFERENCES IN TEXT

The Indian Health Care Improvement Act, referred to in par. (5)(L), is Pub. L. 94-437, Sept. 30, 1976, 90 Stat. 1400, as amended, which is classified principally to chapter 18 (Sec. 1601 et seq.) of Title 25, Indians. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of Title 25 and Tables.

-MISC2-

PRIOR PROVISIONS

A prior section 1171 of act Aug. 14, 1935, was classified to section 1320c-20 of this title prior to repeal by Pub. L. 97-35.

AMENDMENTS

2001 - Par. (5)(D). Pub. L. 107-105 substituted ''Parts A, B, or C'' for ''Part A or part B''.

PURPOSE

Section 261 of title II of Pub. L. 104-191 provided that: ''It is the purpose of this subtitle (subtitle F (Sec. 261-264) of title II of Pub. L. 104-191, enacting this part, amending sections 242k and 1395cc of this title, and enacting provisions set out as a note under section 1320d-2 of this title) to improve the Medicare program under title XVIII of the Social Security Act (subchapter XVIII of this chapter), the medicaid program under title XIX of such Act (subchapter XIX of this chapter), and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.''

-SECREP-

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 1395cc of this title.

-CITE-

42 USC Sec. 1320d-1

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE
CHAPTER 7 - SOCIAL SECURITY
SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE
SIMPLIFICATION
Part C - Administrative Simplification

-HEAD-

Sec. 1320d-1. General requirements for adoption of standards

-STATUTE-

(a) Applicability

Any standard adopted under this part shall apply, in whole or in part, to the following persons:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information

in electronic form in connection with a transaction referred to in section 1320d-2(a)(1) of this title.

(b) Reduction of costs

Any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.

(c) Role of standard setting organizations

(1) In general

Except as provided in paragraph (2), any standard adopted under this part shall be a standard that has been developed, adopted, or modified by a standard setting organization.

(2) Special rules

(A) Different standards

The Secretary may adopt a standard that is different from any standard developed, adopted, or modified by a standard setting organization, if -

(i) the different standard will substantially reduce administrative costs to health care providers and health plans compared to the alternatives; and

(ii) the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5.

(B) No standard by standard setting organization

If no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt under this part -

(i) paragraph (1) shall not apply; and

(ii) subsection (f) of this section shall apply.

(3) Consultation requirement

(A) In general

A standard may not be adopted under this part unless -

(i) in the case of a standard that has been developed, adopted, or modified by a standard setting organization, the organization consulted with each of the organizations described in subparagraph (B) in the course of such development, adoption, or modification; and

(ii) in the case of any other standard, the Secretary, in complying with the requirements of subsection (f) of this section, consulted with each of the organizations described in subparagraph (B) before adopting the standard.

(B) Organizations described

The organizations referred to in subparagraph (A) are the following:

(i) The National Uniform Billing Committee.

(ii) The National Uniform Claim Committee.

(iii) The Workgroup for Electronic Data Interchange.

(iv) The American Dental Association.

(d) Implementation specifications

The Secretary shall establish specifications for implementing each of the standards adopted under this part.

(e) Protection of trade secrets

Except as otherwise required by law, a standard adopted under this part shall not require disclosure of trade secrets or confidential commercial information by a person required to comply with this part.

(f) Assistance to Secretary

In complying with the requirements of this part, the Secretary

shall rely on the recommendations of the National Committee on Vital and Health Statistics established under section 242k(k) of this title, and shall consult with appropriate Federal and State agencies and private organizations. The Secretary shall publish in the Federal Register any recommendation of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.

(g) Application to modifications of standards

This section shall apply to a modification to a standard (including an addition to a standard) adopted under section 1320d-3(b) of this title in the same manner as it applies to an initial standard adopted under section 1320d-3(a) of this title.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1172, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2023.)

-MISC1-

PRIOR PROVISIONS

A prior section 1172 of act Aug. 14, 1935, was classified to section 1320c-21 of this title prior to the general amendment of part B of this subchapter by Pub. L. 97-248.

-SECREP-

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1320d, 1320d-2, 1320d-4, 1320d-7 of this title.

-CITE-

42 USC Sec. 1320d-2

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE
CHAPTER 7 - SOCIAL SECURITY
SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION
Part C - Administrative Simplification

-HEAD-

Sec. 1320d-2. Standards for information transactions and data elements

-STATUTE-

(a) Standards to enable electronic exchange

(1) In general

The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for -

(A) the financial and administrative transactions described in paragraph (2); and

(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

(2) Transactions

The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

- (A) Health claims or equivalent encounter information.
- (B) Health claims attachments.
- (C) Enrollment and disenrollment in a health plan.
- (D) Eligibility for a health plan.
- (E) Health care payment and remittance advice.
- (F) Health plan premium payments.
- (G) First report of injury.
- (H) Health claim status.
- (I) Referral certification and authorization.

(3) Accommodation of specific providers

The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

(b) Unique health identifiers

(1) In general

The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

(2) Use of identifiers

The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

(c) Code sets

(1) In general

The Secretary shall adopt standards that -

(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) of this section from among the code sets that have been developed by private and public entities; or

(B) establish code sets for such data elements if no code sets for the data elements have been developed.

(2) Distribution

The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1320d-3(b) of this title.

(d) Security standards for health information

(1) Security standards

The Secretary shall adopt security standards that -

(A) take into account -

(i) the technical capabilities of record systems used to maintain health information;

(ii) the costs of security measures;

(iii) the need for training persons who have access to health information;

(iv) the value of audit trails in computerized record systems; and

(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that

prevents unauthorized access to such information by such larger organization.

(2) Safeguards

Each person described in section 1320d-1(a) of this title who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards -

(A) to ensure the integrity and confidentiality of the information;

(B) to protect against any reasonably anticipated -

(i) threats or hazards to the security or integrity of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) otherwise to ensure compliance with this part by the officers and employees of such person.

(e) Electronic signature

(1) Standards

The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1) of this section.

(2) Effect of compliance

Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1) of this section.

(f) Transfer of information among health plans

The Secretary shall adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1173, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2024.)

-MISC1-

PRIOR PROVISIONS

A prior section 1173 of act Aug. 14, 1935, was classified to section 1320c-22 of this title prior to the general amendment of part B of this subchapter by Pub. L. 97-248.

RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION

Section 264 of Pub. L. 104-191 directed Secretary of Health and Human Services, in consultation with the National Committee on Vital and Health Statistics and the Attorney General, to submit to Congress, not later than the date that is 12 months after Aug. 21, 1996, detailed recommendations on standards with respect to the privacy of individually identifiable health information, which recommendations were to address at least the rights that an individual who is a subject of individually identifiable health information should have, the procedures that should be established for the exercise of such rights, and the uses and disclosures of such information that should be authorized or required, further provided that if legislation governing such standards was not

enacted by the date that is 36 months after Aug. 21, 1996, the Secretary was to promulgate final regulations containing such standards not later than the date that is 42 months after Aug. 21, 1996, and further provided for preemption of regulations.

-EXEC-

EX. ORD. NO. 13181. TO PROTECT THE PRIVACY OF PROTECTED HEALTH INFORMATION IN OVERSIGHT INVESTIGATIONS

Ex. Ord. No. 13181, Dec. 20, 2000, 65 F.R. 81321, provided:

By the authority vested in me as President of the United States by the Constitution and the laws of the United States of America, it is ordered as follows:

Section 1. Policy.

It shall be the policy of the Government of the United States that law enforcement may not use protected health information concerning an individual that is discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations of a non-health oversight matter, except when the balance of relevant factors weighs clearly in favor of its use. That is, protected health information may not be so used unless the public interest and the need for disclosure clearly outweigh the potential for injury to the patient, to the physician-patient relationship, and to the treatment services. Protecting the privacy of patients' protected health information promotes trust in the health care system. It improves the quality of health care by fostering an environment in which patients can feel more comfortable in providing health care professionals with accurate and detailed information about their personal health. In order to provide greater protections to patients' privacy, the Department of Health and Human Services is issuing final regulations concerning the confidentiality of individually identifiable health information under the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191, see Tables for classification) (HIPAA). HIPAA applies only to "covered entities," such as health care plans, providers, and clearinghouses. HIPAA regulations therefore do not apply to other organizations and individuals that gain access to protected health information, including Federal officials who gain access to health records during health oversight activities.

Under the new HIPAA regulations, health oversight investigators will appropriately have ready access to medical records for oversight purposes. Health oversight investigators generally do not seek access to the medical records of a particular patient, but instead review large numbers of records to determine whether a health care provider or organization is violating the law, such as through fraud against the Medicare system. Access to many health records is often necessary in order to gain enough evidence to detect and bring enforcement actions against fraud in the health care system. Stricter rules apply under the HIPAA regulations, however, when law enforcement officials seek protected health information in order to investigate criminal activity outside of the health oversight realm.

In the course of their efforts to protect the health care system, health oversight investigators may also uncover evidence of wrongdoing unrelated to the health care system, such as evidence of criminal conduct by an individual who has sought health care. For records containing that evidence, the issue thus arises whether the

information should be available for law enforcement purposes under the less restrictive oversight rules or the more restrictive rules that apply to non-oversight criminal investigations.

A similar issue has arisen in other circumstances. Under 18 U.S.C. 3486, an individual's health records obtained for health oversight purposes pursuant to an administrative subpoena may not be used against that individual patient in an unrelated investigation by law enforcement unless a judicial officer finds good cause. Under that statute, a judicial officer determines whether there is good cause by weighing the public interest and the need for disclosure against the potential for injury to the patient, to the physician-patient relationship, and to the treatment services. It is appropriate to extend limitations on the use of health information to all situations in which the government obtains medical records for a health oversight purpose. In recognition of the increasing importance of protecting health information as shown in the medical privacy rule, a higher standard than exists in 18 U.S.C. 3486 is necessary. It is, therefore, the policy of the Government of the United States that law enforcement may not use protected health information concerning an individual, discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations, against that individual except when the balance of relevant factors weighs clearly in favor of its use. That is, protected health information may not be so used unless the public interest and the need for disclosure clearly outweigh the potential for injury to the patient, to the physician-patient relationship, and to the treatment services.

Sec. 2. Definitions.

(a) "Health oversight activities" shall include the oversight activities enumerated in the regulations concerning the confidentiality of individually identifiable health information promulgated by the Secretary of Health and Human Services pursuant to the "Health Insurance Portability and Accountability Act of 1996," as amended (Pub. L. 104-191, see Tables for classification).

(b) "Protected health information" shall have the meaning ascribed to it in the regulations concerning the confidentiality of individually identifiable health information promulgated by the Secretary of Health and Human Services pursuant to the "Health Insurance Portability and Accountability Act of 1996," as amended.

(c) "Injury to the patient" includes injury to the privacy interests of the patient.

Sec. 3. Implementation.

(a) Protected health information concerning an individual patient discovered during the course of health oversight activities shall not be used against that individual patient in an unrelated civil, administrative, or criminal investigation of a non-health oversight matter unless the Deputy Attorney General of the U.S. Department of Justice, or insofar as the protected health information involves members of the Armed Forces, the General Counsel of the U.S. Department of Defense, has authorized such use.

(b) In assessing whether protected health information should be used under subparagraph (a) of this section, the Deputy Attorney General shall permit such use upon concluding that the balance of relevant factors weighs clearly in favor of its use. That is, the Deputy Attorney General shall permit disclosure if the public

interest and the need for disclosure clearly outweigh the potential for injury to the patient, to the physician-patient relationship, and to the treatment services.

(c) Upon the decision to use protected health information under subparagraph (a) of this section, the Deputy Attorney General, in determining the extent to which this information should be used, shall impose appropriate safeguards against unauthorized use.

(d) On an annual basis, the Department of Justice, in consultation with the Department of Health and Human Services, shall provide to the President of the United States a report that includes the following information:

(i) the number of requests made to the Deputy Attorney General for authorization to use protected health information discovered during health oversight activities in a non-health oversight, unrelated investigation;

(ii) the number of requests that were granted as applied for, granted as modified, or denied;

(iii) the agencies that made the applications, and the number of requests made by each agency; and

(iv) the uses for which the protected health information was authorized.

(e) The General Counsel of the U.S. Department of Defense will comply with the requirements of subparagraphs (b), (c), and (d), above. The General Counsel also will prepare a report, consistent with the requirements of subparagraphs (d)(i) through (d)(iv), above, and will forward it to the Department of Justice where it will be incorporated into the Department's annual report to the President.

Sec. 4. Exceptions.

(a) Nothing in this Executive Order shall place a restriction on the derivative use of protected health information that was obtained by a law enforcement agency in a non-health oversight investigation.

(b) Nothing in this Executive Order shall be interpreted to place a restriction on a duty imposed by statute.

(c) Nothing in this Executive Order shall place any additional limitation on the derivative use of health information obtained by the Attorney General pursuant to the provisions of 18 U.S.C. 3486.

(d) This order does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, the officers and employees, or any other person.

William J. Clinton.

-SECRET-

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1320d, 1320d-1, 1320d-3, 1320d-4, 1320d-7, 1396u-2 of this title.

-CITE-

42 USC Sec. 1320d-3

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE

CHAPTER 7 - SOCIAL SECURITY

SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION

Part C - Administrative Simplification

-HEAD-

Sec. 1320d-3. Timetables for adoption of standards

-STATUTE-

(a) Initial standards

The Secretary shall carry out section 1320d-2 of this title not later than 18 months after August 21, 1996, except that standards relating to claims attachments shall be adopted not later than 30 months after August 21, 1996.

(b) Additions and modifications to standards

(1) In general

Except as provided in paragraph (2), the Secretary shall review the standards adopted under section 1320d-2 of this title, and shall adopt modifications to the standards (including additions to the standards), as determined appropriate, but not more frequently than once every 12 months. Any addition or modification to a standard shall be completed in a manner which minimizes the disruption and cost of compliance.

(2) Special rules

(A) First 12-month period

Except with respect to additions and modifications to code sets under subparagraph (B), the Secretary may not adopt any modification to a standard adopted under this part during the 12-month period beginning on the date the standard is initially adopted, unless the Secretary determines that the modification is necessary in order to permit compliance with the standard.

(B) Additions and modifications to code sets

(i) In general

The Secretary shall ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets.

(ii) Additional rules

If a code set is modified under this subsection, the modified code set shall include instructions on how data elements of health information that were encoded prior to the modification may be converted or translated so as to preserve the informational value of the data elements that existed before the modification. Any modification to a code set under this subsection shall be implemented in a manner that minimizes the disruption and cost of complying with such modification.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1174, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2026.)

-SECFREF-

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1320d, 1320d-1, 1320d-2, 1320d-4, 1320d-7 of this title.

-CITE-

42 USC Sec. 1320d-4

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE

CHAPTER 7 - SOCIAL SECURITY
SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE
SIMPLIFICATION
Part C - Administrative Simplification

-HEAD-

Sec. 1320d-4. Requirements

-STATUTE-

(a) Conduct of transactions by plans

(1) In general

If a person desires to conduct a transaction referred to in section 1320d-2(a)(1) of this title with a health plan as a standard transaction -

(A) the health plan may not refuse to conduct such transaction as a standard transaction;

(B) the insurance plan may not delay such transaction, or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the ground that the transaction is a standard transaction; and

(C) the information transmitted and received in connection with the transaction shall be in the form of standard data elements of health information.

(2) Satisfaction of requirements

A health plan may satisfy the requirements under paragraph (1) by -

(A) directly transmitting and receiving standard data elements of health information; or

(B) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse, and receiving standard data elements through the health care clearinghouse.

(3) Timetable for compliance

Paragraph (1) shall not be construed to require a health plan to comply with any standard, implementation specification, or modification to a standard or specification adopted or established by the Secretary under sections 1320d-1 through 1320d-3 of this title at any time prior to the date on which the plan is required to comply with the standard or specification under subsection (b) of this section.

(b) Compliance with standards

(1) Initial compliance

(A) In general

Not later than 24 months after the date on which an initial standard or implementation specification is adopted or established under sections 1320d-1 and 1320d-2 of this title, each person to whom the standard or implementation specification applies shall comply with the standard or specification.

(B) Special rule for small health plans

In the case of a small health plan, paragraph (1) shall be applied by substituting '36 months' for '24 months'. For purposes of this subsection, the Secretary shall determine the plans that qualify as small health plans.

(2) Compliance with modified standards

If the Secretary adopts a modification to a standard or implementation specification under this part, each person to whom

the standard or implementation specification applies shall comply with the modified standard or implementation specification at such time as the Secretary determines appropriate, taking into account the time needed to comply due to the nature and extent of the modification. The time determined appropriate under the preceding sentence may not be earlier than the last day of the 180-day period beginning on the date such modification is adopted. The Secretary may extend the time for compliance for small health plans, if the Secretary determines that such extension is appropriate.

(3) Construction

Nothing in this subsection shall be construed to prohibit any person from complying with a standard or specification by -

(A) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse; or

(B) receiving standard data elements through a health care clearinghouse.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1175, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2027.)

-MISC1-

EXTENSION OF DEADLINE FOR COVERED ENTITIES SUBMITTING COMPLIANCE PLANS

Pub. L. 107-105, Sec. 2, Dec. 27, 2001, 115 Stat. 1003, provided that:

''(a) In General. -

''(1) Extension. - Subject to paragraph (2), notwithstanding section 1175(b)(1)(A) of the Social Security Act (42 U.S.C. 1320d-4(b)(1)(A)) and section 162.900 of title 45, Code of Federal Regulations, a health care provider, health plan (other than a small health plan), or a health care clearinghouse shall not be considered to be in noncompliance with the applicable requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations, before October 16, 2003.

''(2) Condition. - Paragraph (1) shall apply to a person described in such paragraph only if, before October 16, 2002, the person submits to the Secretary of Health and Human Services a plan of how the person will come into compliance with the requirements described in such paragraph not later than October 16, 2003. Such plan shall be a summary of the following:

''(A) An analysis reflecting the extent to which, and the reasons why, the person is not in compliance.

''(B) A budget, schedule, work plan, and implementation strategy for achieving compliance.

''(C) Whether the person plans to use or might use a contractor or other vendor to assist the person in achieving compliance.

''(D) A timeframe for testing that begins not later than April 16, 2003.

''(3) Electronic submission. - Plans described in paragraph (2) may be submitted electronically.

''(4) Model form. - Not later than March 31, 2002, the Secretary of Health and Human Services shall promulgate a model form that persons may use in drafting a plan described in

paragraph (2). The promulgation of such form shall be made without regard to chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act').

''(5) Analysis of plans; reports on solutions. -

''(A) Analysis of plans. -

''(i) Furnishing of plans. - Subject to subparagraph (D), the Secretary of Health and Human Services shall furnish the National Committee on Vital and Health Statistics with a sample of the plans submitted under paragraph (2) for analysis by such Committee.

''(ii) Analysis. - The National Committee on Vital and Health Statistics shall analyze the sample of the plans furnished under clause (i).

''(B) Reports on solutions. - The National Committee on Vital and Health Statistics shall regularly publish, and widely disseminate to the public, reports containing effective solutions to compliance problems identified in the plans analyzed under subparagraph (A). Such reports shall not relate specifically to any one plan but shall be written for the purpose of assisting the maximum number of persons to come into compliance by addressing the most common or challenging problems encountered by persons submitting such plans.

''(C) Consultation. - In carrying out this paragraph, the National Committee on Vital and Health Statistics shall consult with each organization -

''(i) described in section 1172(c)(3)(B) of the Social Security Act (42 U.S.C. 1320d-1(c)(3)(B)); or

''(ii) designated by the Secretary of Health and Human Services under section 162.910(a) of title 45, Code of Federal Regulations.

''(D) Protection of confidential information. -

''(i) In general. - The Secretary of Health and Human Services shall ensure that any material provided under subparagraph (A) to the National Committee on Vital and Health Statistics or any organization described in subparagraph (C) is redacted so as to prevent the disclosure of any -

''(I) trade secrets;

''(II) commercial or financial information that is privileged or confidential; and

''(III) other information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

''(ii) Construction. - Nothing in clause (i) shall be construed to affect the application of section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act'), including the exceptions from disclosure provided under subsection (b) of such section.

''(6) Enforcement through exclusion from participation in medicare. -

''(A) In general. - In the case of a person described in paragraph (1) who fails to submit a plan in accordance with paragraph (2), and who is not in compliance with the applicable requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations, on or after October 16, 2002, the person may be excluded at the discretion of the Secretary of Health and Human Services from participation (including under part C or as a contractor under sections 1816, 1842, and 1893)

(42 U.S.C. 1395h, 1395u, 1395ddd) in title XVIII of the Social Security Act (42 U.S.C. 1395 et seq.).

''(B) Procedure. - The provisions of section 1128A of the Social Security Act (42 U.S.C. 1320a-7a) (other than the first and second sentences of subsection (a) and subsection (b)) shall apply to an exclusion under this paragraph in the same manner as such provisions apply with respect to an exclusion or proceeding under section 1128A(a) of such Act.

''(C) Construction. - The availability of an exclusion under this paragraph shall not be construed to affect the imposition of penalties under section 1176 of the Social Security Act (42 U.S.C. 1320d-5).

''(D) Nonapplicability to complying persons. - The exclusion under subparagraph (A) shall not apply to a person who -

''(i) submits a plan in accordance with paragraph (2); or

''(ii) who is in compliance with the applicable requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations, on or before October 16, 2002.

''(b) Special Rules. -

''(1) Rules of construction. - Nothing in this section shall be construed -

''(A) as modifying the October 16, 2003, deadline for a small health plan to comply with the requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations; or

''(B) as modifying -

''(i) the April 14, 2003, deadline for a health care provider, a health plan (other than a small health plan), or a health care clearinghouse to comply with the requirements of subpart E of part 164 of title 45, Code of Federal Regulations; or

''(ii) the April 14, 2004, deadline for a small health plan to comply with the requirements of such subpart.

''(2) Applicability of privacy standards before compliance deadline for information transaction standards. -

''(A) In general. - Notwithstanding any other provision of law, during the period that begins on April 14, 2003, and ends on October 16, 2003, a health care provider or, subject to subparagraph (B), a health care clearinghouse, that transmits any health information in electronic form in connection with a transaction described in subparagraph (C) shall comply with the requirements of subpart E of part 164 of title 45, Code of Federal Regulations, without regard to whether the transmission meets the standards required by part 162 of such title.

''(B) Application to health care clearinghouses. - For purposes of this paragraph, during the period described in subparagraph (A), an entity that processes or facilitates the processing of information in connection with a transaction described in subparagraph (C) and that otherwise would be treated as a health care clearinghouse shall be treated as a health care clearinghouse without regard to whether the processing or facilitation produces (or is required to produce) standard data elements or a standard transaction as required by part 162 of title 45, Code of Federal Regulations.

''(C) Transactions described. - The transactions described in this subparagraph are the following:

''(i) A health care claims or equivalent encounter

information transaction.

''(ii) A health care payment and remittance advice transaction.

''(iii) A coordination of benefits transaction.

''(iv) A health care claim status transaction.

''(v) An enrollment and disenrollment in a health plan transaction.

''(vi) An eligibility for a health plan transaction.

''(vii) A health plan premium payments transaction.

''(viii) A referral certification and authorization transaction.

''(c) Definitions. - In this section -

''(1) the terms 'health care provider', 'health plan', and 'health care clearinghouse' have the meaning given those terms in section 1171 of the Social Security Act (42 U.S.C. 1320d) and section 160.103 of title 45, Code of Federal Regulations;

''(2) the terms 'small health plan' and 'transaction' have the meaning given those terms in section 160.103 of title 45, Code of Federal Regulations; and

''(3) the terms 'health care claims or equivalent encounter information transaction', 'health care payment and remittance advice transaction', 'coordination of benefits transaction', 'health care claim status transaction', 'enrollment and disenrollment in a health plan transaction', 'eligibility for a health plan transaction', 'health plan premium payments transaction', and 'referral certification and authorization transaction' have the meanings given those terms in sections 162.1101, 162.1601, 162.1801, 162.1401, 162.1501, 162.1201, 162.1701, and 162.1301 of title 45, Code of Federal Regulations, respectively.''

-CITE-

42 USC Sec. 1320d-5

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE

CHAPTER 7 - SOCIAL SECURITY

SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION

Part C - Administrative Simplification

-HEAD-

Sec. 1320d-5. General penalty for failure to comply with requirements and standards

-STATUTE-

(a) General penalty

(1) In general

Except as provided in subsection (b) of this section, the Secretary shall impose on any person who violates a provision of this part a penalty of not more than \$100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000.

(2) Procedures

The provisions of section 1320a-7a of this title (other than subsections (a) and (b) and the second sentence of subsection

(f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1320a-7a of this title.

(b) Limitations

(1) Offenses otherwise punishable

A penalty may not be imposed under subsection (a) of this section with respect to an act if the act constitutes an offense punishable under section 1320d-6 of this title.

(2) Noncompliance not discovered

A penalty may not be imposed under subsection (a) of this section with respect to a provision of this part if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.

(3) Failures due to reasonable cause

(A) In general

Except as provided in subparagraph (B), a penalty may not be imposed under subsection (a) of this section if -

(i) the failure to comply was due to reasonable cause and not to willful neglect; and

(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

(B) Extension of period

(i) No penalty

The period referred to in subparagraph (A)(ii) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure to comply.

(ii) Assistance

If the Secretary determines that a person failed to comply because the person was unable to comply, the Secretary may provide technical assistance to the person during the period described in subparagraph (A)(ii). Such assistance shall be provided in any manner determined appropriate by the Secretary.

(4) Reduction

In the case of a failure to comply which is due to reasonable cause and not to willful neglect, any penalty under subsection (a) of this section that is not entirely waived under paragraph (3) may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1176, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2028.)

-CITE-

42 USC Sec. 1320d-6

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE
CHAPTER 7 - SOCIAL SECURITY
SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE
SIMPLIFICATION

Part C - Administrative Simplification

-HEAD-

Sec. 1320d-6. Wrongful disclosure of individually identifiable health information

-STATUTE-

(a) Offense

A person who knowingly and in violation of this part -

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b) of this section.

(b) Penalties

A person described in subsection (a) of this section shall -

(1) be fined not more than \$50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and

(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1177, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2029.)

-SECFREF-

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 1320d-5 of this title.

-CITE-

42 USC Sec. 1320d-7

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE

CHAPTER 7 - SOCIAL SECURITY

SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION

Part C - Administrative Simplification

-HEAD-

Sec. 1320d-7. Effect on State law

-STATUTE-

(a) General effect

(1) General rule

Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1320d-1 through 1320d-3 of this title, shall supersede any contrary provision of State law, including a provision of State law that requires medical or

health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

(2) Exceptions

A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1320d-1 through 1320d-3 of this title, shall not supersede a contrary provision of State law, if the provision of State law -

(A) is a provision the Secretary determines -

(i) is necessary -

(I) to prevent fraud and abuse;

(II) to ensure appropriate State regulation of insurance and health plans;

(III) for State reporting on health care delivery or costs; or

(IV) for other purposes; or

(ii) addresses controlled substances; or

(B) subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.

(b) Public health

Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

(c) State regulatory reporting

Nothing in this part shall limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1178, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2029.)

-REFTEXT-

REFERENCES IN TEXT

Section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, referred to in subsec. (a)(2)(B), is section 264(c)(2) of Pub. L. 104-191, which is set out as a note under section 1320d-2 of this title.

-CITE-

42 USC Sec. 1320d-8

01/22/02

-EXPCITE-

TITLE 42 - THE PUBLIC HEALTH AND WELFARE
CHAPTER 7 - SOCIAL SECURITY
SUBCHAPTER XI - GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION
Part C - Administrative Simplification

-HEAD-

Sec. 1320d-8. Processing payment transactions by financial institutions

-STATUTE-

To the extent that an entity is engaged in activities of a financial institution (as defined in section 3401 of title 12), or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.

(2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph

(1) -

(A) for transferring receivables;

(B) for auditing;

(C) in connection with -

(i) a customer dispute; or

(ii) an inquiry from, or to, a customer;

(D) in a communication to a customer of the entity regarding the customer's transactions, payment card, account, check, or electronic funds transfer;

(E) for reporting to consumer reporting agencies; or

(F) for complying with -

(i) a civil or criminal subpoena; or

(ii) a Federal or State law regulating the entity.

-SOURCE-

(Aug. 14, 1935, ch. 531, title XI, Sec. 1179, as added Pub. L. 104-191, title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2030.)

§ 164.102

- 164.528 Accounting of disclosures of protected health information.
164.530 Administrative requirements.
164.532 Transition provisions.
164.534 Compliance dates for initial implementation of the privacy standards.

AUTHORITY: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d-1320d-8), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, and 42 U.S.C. 1320d-2 and 1320d-4, sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)).

SOURCE: 65 FR 82802, Dec. 28, 2000, unless otherwise noted.

Subpart A—General Provisions

§ 164.102 Statutory basis.

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

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002]

§ 164.103 Definitions.

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

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

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

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

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(C).

Hybrid entity means a single legal entity:

- (1) That is a covered entity;
- (2) Whose business activities include both covered and non-covered functions; and
- (3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(C).

45 CFR Subtitle A (10-1-03 Edition)

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

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

[68 FR 8374, Feb. 20, 2003]

§ 164.104 Applicability.

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

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

(b) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, or other than as a business associate of a covered entity, the clearinghouse must comply with § 164.105 relating to organizational requirements for covered entities, including the designation of health care components of a covered entity.

[68 FR 8375, Feb. 20, 2003]

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of subparts C and E of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care

component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*

(i) *Application of other provisions.* In applying a provision of subparts C and E of this part, other than the requirements of this section, §164.314, and §164.504, to a hybrid entity:

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

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

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

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

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this section and subparts C and E of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

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

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by subpart E of this part;

(D) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section that creates, receives, maintains, or transmits electronic protected health information on behalf of the health care component is in compliance with subpart C of this part; and

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

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

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

(B) The covered entity is responsible for complying with §164.316(a) and §164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this section and subparts C and E of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

§ 164.106

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

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of subparts C and E of this part.

(1) *Implementation specifications:*

(i) *Requirements for designation of an affiliated covered entity.* (A) 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 subparts C and E of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that:

(A) The affiliated covered entity's creation, receipt, maintenance, or transmission of electronic protected health information complies with the applicable requirements of subpart C of this part;

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

(C) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

(c)(1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation as required by paragraph (c)(1) of this section for 6 years from the date of its creation or

45 CFR Subtitle A (10–1–03 Edition)

the date when it last was in effect, whichever is later.

[68 FR 8375, Feb. 20, 2003]

§ 164.106 Relationship to other parts.

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

Subpart B [Reserved]

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

AUTHORITY: 42 U.S.C. 1320d-2 and 1320d-4.

SOURCE: 68 FR 8376, Feb. 20, 2003, unless otherwise noted.

§ 164.302 Applicability.

A covered entity must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information.

§ 164.304 Definitions.

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

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subpart E of this part.)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into

a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) *Flexibility of approach.* (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) *Standards.* A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications.*

In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.

§ 164.308

45 CFR Subtitle A (10–1–03 Edition)

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s electronic protected health information; and

(ii) As applicable to the entity—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) *Maintenance.* Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003]

§ 164.308 **Administrative safeguards.**

(a) A covered entity must, in accordance with § 164.306:

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) *Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3)(i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) *Standard: Information access management.* Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications:*

(A) *Isolating health care clearinghouse functions* (Required). If a health care

clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5)(i) *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications*. Implement:

(A) *Security reminders* (Addressable). Periodic security updates.

(B) *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6)(i) *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

(ii) *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

(7)(i) *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages

systems that contain electronic protected health information.

(ii) *Implementation specifications*:

(A) *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) *Standard: Evaluation*. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

(b)(1) *Standard: Business associate contracts and other arrangements*. A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

(2) This standard does not apply with respect to—

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a

§ 164.310

group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) *Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

§ 164.310 Physical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) *Implementation specifications:*

(i) *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) *Facility security plan* (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor con-

45 CFR Subtitle A (10–1–03 Edition)

trol, and control of access to software programs for testing and revision.

(iv) *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) *Implementation specifications:*

(i) *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§ 164.312 Technical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) *Standard: Access control*. Implement technical policies and procedures for electronic information systems

that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) *Implementation specifications:*

(i) *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls* (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is

not improperly modified without detection until disposed of.

(ii) *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements.*

(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

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

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

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

(2) *Implementation specifications* (Required).

(i) *Business associate contracts*. The contract between a covered entity and a business associate must provide that the business associate will—

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

§ 164.316

45 CFR Subtitle A (10–1–03 Edition)

(D) 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.

(ii) *Other arrangements.* (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if—

(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or

(2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.

(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in §160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

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

(b)(1) *Standard: Requirements for group health plans.* Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appro-

priately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation specifications* (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

§ 164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with §164.306:

(a) *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) *Standard: Documentation.* (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications:*

(i) *Time limit* (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability* (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates* (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

§ 164.318 Compliance dates for the initial implementation of the security standards.

(a) *Health plan.* (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

APPENDIX A TO SUBPART C OF PART 164—SECURITY STANDARDS: MATRIX

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A)
Evaluation	164.308(a)(8)	Applications and Data Criticality Analysis (A)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	(R) Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

§ 164.500

45 CFR Subtitle A (10–1–03 Edition)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A) (R)
Audit Controls	164.312(b)	Mechanism to Authenticate Electronic Protected Health Information (A) (R)
Integrity	164.312(c)(1)	
Person or Entity Authentication	164.312(d)	Integrity Controls (A) Encryption (A)
Transmission Security	164.312(e)(1)	

Subpart D [Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

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

§ 164.500 Applicability.

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

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

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

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

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

(iv) Section 164.504 relating to the organizational requirements for covered entities;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to

agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

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

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

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

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003]

§ 164.501 Definitions.

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

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with

or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

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

Designated record set means:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 164.501

(iii) Resolution of internal grievances;

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

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

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

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

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

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

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

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

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

45 CFR Subtitle A (10–1–03 Edition)

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

Marketing means:

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

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

(ii) For treatment of the individual; or

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

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

Payment means:

(1) The activities undertaken by:

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

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

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

(i) Determinations of eligibility or coverage (including coordination of

benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

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

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

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

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

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

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

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

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of

such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

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

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

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003]

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

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

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

- (i) To the individual;
- (ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;
- (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of § 164.502(b), § 164.514(d), and § 164.530(c) with respect to such otherwise permitted or required use or disclosure;
- (iv) Pursuant to and in compliance with a valid authorization under § 164.508;
- (v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
- (vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), or (g).

§ 164.502

45 CFR Subtitle A (10-1-03 Edition)

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

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

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

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

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

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

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

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

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

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

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

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

(d) *Standard: Uses and disclosures of de-identified protected health information.*(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health infor-

mation only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

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

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

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

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

(ii) This standard does not apply:

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

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

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering

the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

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

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

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

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

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

(3)(i) *Implementation specification: unemancipated minors.* If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except

that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

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

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

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

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

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

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

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

§ 164.504

such decision must be made by a licensed health care professional, in the exercise of professional judgment.

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

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

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

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

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

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

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

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

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims.* (1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this

45 CFR Subtitle A (10–1–03 Edition)

subpart if a member of its workforce or a business associate discloses protected health information, provided that:

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

(ii) The disclosure is to:

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

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

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

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

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

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002]

§ 164.504 Uses and disclosures: Organizational requirements.

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

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

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

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

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

(b)-(d)

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

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

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

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

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

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

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

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

(ii) Provide that the business associate will:

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

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

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

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

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

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

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

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

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

§ 164.504

45 CFR Subtitle A (10-1-03 Edition)

disclosures to those purposes that make the return or destruction of the information infeasible.

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

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

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

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

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

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

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the

information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

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

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

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

(A) The disclosure is required by law; or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) Disclose protected health information to a plan sponsor to carry out plan

§ 164.506

45 CFR Subtitle A (10–1–03 Edition)

administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

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

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

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

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

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003]

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

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

this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.* (1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

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

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

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

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

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

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

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

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

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates

in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

[67 FR 53268, Aug. 14, 2002]

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

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

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

(i) To carry out the following treatment, payment, or health care operations:

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

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

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

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

(3) *Authorization required: Marketing.*

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

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

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

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

(b) *Implementation specifications: general requirements—(1) Valid authorizations.* (i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

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

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

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

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

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

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

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

(i) An authorization for the use or disclosure of protected health information for a research study 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;

§ 164.508

45 CFR Subtitle A (10-1-03 Edition)

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

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

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

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

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

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

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

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

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

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

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

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

(c) *Implementation specifications: Core elements and requirements—(1) Core elements.* A valid authorization under this section must contain at least the following elements:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[67 FR 53268, Aug. 14, 2002]

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

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered enti-

ty may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

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

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

(A) The individual's name;

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

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

(D) The individual's religious affiliation; and

(ii) Disclose for directory purposes such information:

(A) To members of the clergy; or

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

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

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

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

(B) In the individual's best interest as determined by the covered health

§ 164.512

45 CFR Subtitle A (10–1–03 Edition)

care provider, in the exercise of professional judgment.

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

(b) *Standard: uses and disclosures for involvement in the individual's care and notification purposes.* (1) *Permitted uses and disclosures.* (i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

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

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

(i) Obtains the individual's agreement;

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

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

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the oppor-

tunity 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.

(4) *Use and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002]

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

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

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

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

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

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

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

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

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

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been

recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

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

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

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

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

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

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

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

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

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

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

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases

§ 164.512

45 CFR Subtitle A (10-1-03 Edition)

in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: Disclosures about victims of abuse, neglect or domestic violence.* (1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

- (i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
- (ii) If the individual agrees to the disclosure; or
- (iii) To the extent the disclosure is expressly authorized by statute or regulation and:

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

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

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

- (i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- (ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes

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

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

- (i) The health care system;
- (ii) Government benefit programs for which health information is relevant to beneficiary eligibility;
- (iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- (iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

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

- (i) The receipt of health care;
- (ii) A claim for public benefits related to health; or
- (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

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

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

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

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

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

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

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

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

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

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

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

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

(1) No objections were filed; or

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

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

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

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

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

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

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

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

§ 164.512

45 CFR Subtitle A (10-1-03 Edition)

meet the requirements of paragraph (e)(1)(iv) of this section.

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

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

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

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

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

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

(B) A grand jury subpoena; or

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

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

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

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

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

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

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

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

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

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

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

(i) The individual agrees to the disclosure; or

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

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

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

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

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

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

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

(A) The commission and nature of a crime;

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

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

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

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

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

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

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

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

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in

§ 164.512

45 CFR Subtitle A (10-1-03 Edition)

which the member has a conflict of interest.

(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) *Research on decedent's information.* The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(1) An adequate plan to protect the identifiers from improper use and disclosure;

(2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the re-

search, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph

(i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) *Standard: Uses and disclosures to avert a serious threat to health or safety.*

(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

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

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

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

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to para-

graph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: Uses and disclosures for specialized government functions.* (1) *Military and veterans activities.* (i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Transportation may disclose

to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the FEDERAL REGISTER pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (*e.g.*, Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Depart-

ment of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations.* (i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; and

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.* (i) A health plan that is a government program providing public benefits may

disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) *Standard: Disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002]

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

(a) *Standard: de-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally

accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

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

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

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

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

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

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

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

§ 164.514

45 CFR Subtitle A (10–1–03 Edition)

(O) Internet Protocol (IP) address numbers;

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

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

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

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

(c) *Implementation specifications: re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) *Standard: minimum necessary requirements.* In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) *Implementation specifications: minimum necessary uses of protected health information.* (i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in

paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) *Implementation specification: Minimum necessary disclosures of protected health information.* (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

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

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: Minimum necessary requests for protected health information.* (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made,

when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

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

(5) *Implementation specification: Other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- (i) Names;
- (ii) Postal address information, other than town or city, State, and zip code;
- (iii) Telephone numbers;
- (iv) Fax numbers;
- (v) Electronic mail addresses;
- (vi) Social security numbers;
- (vii) Medical record numbers;
- (viii) Health plan beneficiary numbers;
- (ix) Account numbers;

- (x) Certificate/license numbers;

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

- (xii) Device identifiers and serial numbers;

- (xiii) Web Universal Resource Locators (URLs);

- (xiv) Internet Protocol (IP) address numbers;

- (xv) Biometric identifiers, including finger and voice prints; and

- (xvi) Full face photographic images and any comparable images.

(3) *Implementation specification: Permitted purposes for uses and disclosures.*

(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) *Implementation specifications: Data use agreement.—(i) Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

§ 164.514

45 CFR Subtitle A (10–1–03 Edition)

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

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

(4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(5) Not identify the information or contact the individuals.

(iii) *Compliance.* (A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

(f)(1) *Standard: Uses and disclosures for fundraising.* A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual; and

(ii) Dates of health care provided to an individual.

(2) *Implementation specifications: Fundraising requirements.* (i) The covered entity may not use or disclose

protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice;

(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: Verification.* (i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable

under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand

jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002]

§ 164.520 Notice of privacy practices for protected health information.

(a) *Standard: notice of privacy practices—(1) Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Exception for group health plans.* (i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

§ 164.520

45 CFR Subtitle A (10–1–03 Edition)

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in §164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) *Implementation specifications: content of notice—(1) Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”

(ii) *Uses and disclosures.* The notice must contain:

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

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual’s written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such

use or disclosure must reflect the more stringent law as defined in §160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A statement that other uses and disclosures will be made only with the individual’s written authorization and that the individual may revoke such authorization as provided by §164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:

(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;

(B) The covered entity may contact the individual to raise funds for the covered entity; or

(C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

(iv) *Individual rights.* The notice must contain a statement of the individual’s rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by §164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;

(B) The right to receive confidential communications of protected health information as provided by §164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by §164.524;

(D) The right to amend protected health information as provided by §164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by §164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

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

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with §164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

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

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by §164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) *Optional elements.* (i) In addition to the information required by paragraph

(b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by §164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with §164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) *Specific requirements for health plans.* (i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and

(C) Within 60 days of a material revision to the notice, to individuals then covered by the plan.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which

§ 164.520

45 CFR Subtitle A (10-1-03 Edition)

coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.* (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: Joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by §164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

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

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.* (i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under §164.510(b).

(ii) A covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected

health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§164.502(a)(2)(ii), 164.510(a) or 164.512.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate its agreement to a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity that agrees to a restriction must document the restriction in accordance with §164.530(j).

(b)(1) *Standard: Confidential communications requirements.* (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all

§ 164.524

or part of that information could endanger the individual.

(2) *Implementation specifications: Conditions on providing confidential communications.*

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

§ 164.524 Access of individuals to protected health information.

(a) *Standard: Access to protected health information.* (1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

45 CFR Subtitle A (10–1–03 Edition)

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

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

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

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

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

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4)

of this section, in the following circumstances:

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

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

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: requests for access and timely action.* (1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity.*

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must in-

form the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

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

§ 164.524

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

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

(A) The individual agrees in advance to such a summary or explanation; and

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

(3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

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

(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;

(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

45 CFR Subtitle A (10-1-03 Edition)

(d) *Implementation specifications: Denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

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

(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in §164.530(d) or to the Secretary pursuant to the procedures in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

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

(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide

written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

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

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

§ 164.526 Amendment of protected health information.

(a) *Standard: Right to amend.* (1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

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

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

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: requests for amendment and timely action.*

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

(2) *Timely action by the covered entity.*

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

§ 164.526

45 CFR Subtitle A (10–1–03 Edition)

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

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

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

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in §164.530(d) or to the Secretary pursuant to the procedures established in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested

amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

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

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.* (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment.* A covered

entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.* (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.506;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;

(iv) Pursuant to an authorization as provided in § 164.508;

(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

(viii) As part of a limited data set in accordance with § 164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides

the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: Content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a

§ 164.528

45 CFR Subtitle A (10–1–03 Edition)

disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health infor-

mation of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) *Implementation specifications: Provision of the accounting.* (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

§ 164.530 Administrative requirements.

(a)(1) *Standard: Personnel designations.*

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) *Implementation specification: Personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

(2) *Implementation specifications: Training.* (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been

provided, as required by paragraph (j) of this section.

(c)(1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) *Implementation specification: Safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: Documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) *Standard: Mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

§ 164.530

45 CFR Subtitle A (10–1–03 Edition)

(g) *Standard: Refraining from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(1) *Individuals.* Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) *Individuals and others.* Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) *Standard: Waiver of rights.* A covered entity may not require individuals to waive their rights under §160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

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

(2) *Standard: Changes to policies or procedures.* (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the

standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in §164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with §164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) *Implementation specification: Changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by §164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with §164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: Changes to privacy practices stated in the notice.* (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by §164.520(b)(3) to state the changed practice and make the revised notice available as required by §164.520(c). The covered entity may not implement a change to a policy or procedure prior

to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)–(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: Changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: Documentation.* A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or

the date when it last was in effect, whichever is later.

(k) *Standard: Group health plans.* (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002]

§ 164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart 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

§ 164.532

45 CFR Subtitle A (10–1–03 Edition)

disclosure and there is no agreed-to restriction in accordance with § 164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research; or

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research.

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this subpart, a covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does

not comply with §§ 164.502(e) and 164.504(e) consistent with the requirements, and only for such time, set forth in paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance— (1) Qualification.* Notwithstanding other sections of this subpart, a covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements of §§ 164.502(e) and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to October 15, 2002, such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; and

(ii) The contract or other arrangement is not renewed or modified from October 15, 2002, until the compliance date set forth in § 164.534.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section, shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after the compliance date set forth in § 164.534; or

(ii) April 14, 2004.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002]

Department of Health and Human Services

§ 164.534

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following as applicable:

(1) *Health plans other than small health plans.* April 14, 2003.

(2) *Small health plans.* April 14, 2004.

(c) *Health clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

[66 FR 12434, Feb. 26, 2001]

PARTS 165–199 [RESERVED]