October 29, 1999

For the reasons set forth in the preamble, it is proposed to amend 45 CFR subtitle A by adding a new subchapter C, consisting of parts 160 through 164, to read as follows:

SUBCHAPTER C - ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS

PART

160 -- GENERAL ADMINISTRATIVE REQUIREMENTS

161-163 – [RESERVED]

164 – SECURITY AND PRIVACY

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A – General Provisions

Sec.

Subpart B – Preemption of State Law

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

Subpart A - General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act, as amended, which require HHS to adopt national standards to enable the electronic exchange of health information in the health care system. The requirements of this subchapter also implement section 264 of Pub. L 104-191, which requires that HHS adopt national standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a)(1) of the Social Security Act. The purpose of these provisions is to promote administrative simplification.

§ 160.102 Applicability.

Except as otherwise provided, the standards, requirements, and implementation specifications adopted or designated under the parts of this subchapter apply to any entity that is:

(a) A health plan;

(b) A health care clearinghouse; and

(c) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act, as amended.

Covered entity means an entity described in § 160.102.

Health care means the provision of care, services, or supplies to a patient and includes any:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body;

(2) Sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or

(3) Procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

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. The entity receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended payer or payers, and forwards the processed transaction to appropriate payers and clearinghouses. Billing services, repricing companies, community health management information systems, community health information systems, and "value-added" networks and switches are considered to be health care clearinghouses for purposes of this part, if they perform the functions of health care clearinghouses as described in the preceding sentences.

Health care provider means a provider of services as defined in section 1861(u) of the Act, a provider of medical or health services as defined in section 1861(s) of the Act, and any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

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

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

Health plan means an individual or group plan that provides, or pays the cost of, medical care. Such term includes, when applied to government funded or assisted programs, the components of the government agency administering the program. "Health plan" includes the following, singly or in combination:

(1) A group health plan, defined as an employee welfare benefit plan (as currently defined in section 3(1) of the Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance or otherwise, that:

(i) Has 50 or more participants; or

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

(2) A health insurance issuer, defined as an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State or other law that regulates insurance.

(3) A health maintenance organization, defined as a federally qualified health maintenance organization, an organization recognized as a health maintenance organization under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such a health maintenance organization.

(4) Part A or Part B of the Medicare program under title XVIII of the Act.

(5) The Medicaid program under title XIX of the Act.

(6) A Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss).

(7) A long-term care policy, including a nursing home fixed-indemnity policy.

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

(9) The health care program for active military personnel under title 10 of the United States Code.

(10) The veterans health care program under 38 U.S.C. chapter 17.

(11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in 10 U.S.C. 1072(4).

(12) The Indian Health Service program under the Indian Health Care Improvement Act (25 U.S.C. 1601, et seq.).

(13) The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89.

(14) An approved State child health plan for child health assistance that meets the requirements of section 2103 of the Act.

(15) A Medicare Plus Choice organization as defined in 42 CFR 422.2, with a contract under 42 CFR part 422, subpart K.

(16) Any other individual or group health plan, or combination thereof, that provides or pays for the cost of medical care.

Secretary means the Secretary of Health and Human Services and any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a prescribed set of rules, conditions, or requirements concerning classification of components, specification of materials, performance or operations, or delineation of procedures, in describing products, systems, services or practices.

State includes the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Transaction means the exchange of information between two parties to carry out financial or administrative activities related to health care. It includes the following:

(1) Health claims or equivalent encounter information;

(2) Health care payment and remittance advice;

(3) Coordination of benefits;

(4) Health claims status;

(5) Enrollment and disenrollment in a health plan;

(6) Eligibility for a health plan;
(7) Health plan premium payments;
(8) Referral certification and authorization;
(9) First report of injury;
(10) Health claims attachments; and
(11) Other transactions as the Secretary may prescribe by regulation.

§ 160.104 Effective dates of a modification to a standard or implementation specification.

The Secretary may modify a standard or implementation specification after the first year in which the standard or implementation specification is required to be used, but not more frequently than once every 12 months. If the Secretary adopts a modification to a standard or implementation specification, the implementation date of the modified standard or implementation specification may be no earlier than 180 days following the adoption of the modification. The Secretary will determine the actual date, taking into account the time needed to comply due to the nature and extent of the modification. The Secretary may extend the time for compliance for small health plans.

Subpart B – Preemption of State Law

§ 160.201 Applicability.

The provisions of this subpart apply to determinations and advisory opinions issued by the Secretary pursuant to 42 U.S.C. 1320d-7.

§ 160.202 Definitions.

For the purpose of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A party would find it impossible to comply with both the State and federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.

More stringent means, 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 law which meets one or more of the following criteria, as applicable:

(1) With respect to a use or disclosure, provides a more limited use or disclosure (in terms of the number of potential recipients of the information, the amount of information to be disclosed, or the circumstances under which information may be disclosed).

(2) With respect to the rights of individuals of access to or amendment of individually identifiable health information, permits greater rights or access or amendment, as applicable, provided, however, that nothing in this subchapter shall be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information regarding a minor to a parent, guardian or person acting in loco parentis of such minor.

(3) With respect to penalties, provides greater penalties.

(4) With respect to information to be provided to an individual about a proposed use, disclosure, rights, remedies, and similar issues, provides the greater amount of information.

(5) With respect to form or substance of authorizations for use or disclosure of information, provides requirements that narrow the scope or duration, increase the difficulty of obtaining, or reduce the coercive effect of the circumstances surrounding the authorization.

(6) With respect to recordkeeping or accounting requirements, provides for the retention or reporting of more detailed information or for a longer duration.

(7) With respect to any other matter, provides greater privacy protection for the individual.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or the effect of affecting the privacy of health information in a direct, clear, and substantial way.

State law means a law, decision, rule, regulation, or other State action having the effect of law.

§ 160.203 General rule and exceptions.

General rule. A standard, requirement, or implementation specification adopted under or pursuant to this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except where one or more of the following conditions is met:

(a) A determination is made by the Secretary pursuant to § 160.204(a) that the provision of State law:

(1) 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 related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system; or

(2) Addresses controlled substances.

(b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, or the State established procedures, are established under a State law providing for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

§ 160.204 Process for requesting exception determinations or advisory opinions.

(a) Determinations.

(1) A State may submit a written request to the Secretary to except a provision of State law from preemption under § 160.203(a). The request must include the following information:

(i) The State law for which the exception is requested;
(ii) The particular standard(s), requirement(s), or implementation specification(s) for which the exception is requested;
(iii) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
(iv) How health care providers, health plans, and other entities would be affected by the exception;
(v) The length of time for which the exception would be in effect, if less than three years;
(vi) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at §160.203(a); and
(vii) Any other information the Secretary may request in order to make the determination.
(2) Requests for exception under this section must be submitted to the Secretary at an address which will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.
(3) The Secretary's determination under this paragraph will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met. If it is determined that the federal standard, requirement, or implementation specification accomplishes the purposes of the criterion or criteria at § 160.203(a) as well as or better than the State law for which the request is made, the request will be denied.
(4) An exception granted under this paragraph is effective for three years or for such lesser time as is specified in the determination granting the request.
(5) If an exception is granted under this paragraph, the exception has effect only with respect to transactions taking place wholly within the State for which the exception was requested.
(6) Any change to the standard, requirement, or implementation specification or provision of State law upon which an exception was granted requires a new request for an exception. Absent such a request and a favorable determination thereon, the standard, requirement, or implementation specification remains in effect. The responsibility for recognizing the need for and making the request lies with the original requestor.
(7) The Secretary may seek changes to a standard, requirement, or implementation specification based on requested exceptions or may urge the requesting State or other organizations or persons to do so.
(8) Determinations made by the Secretary pursuant to this paragraph will be published annually in the Federal Register.
(b) Advisory opinions.
(1) The Secretary may issue advisory opinions as to whether a provision of State law constitutes an exception under § 160.203(b) to the general rule of preemption under that section. The Secretary may issue such opinions at the request of a State or at the Secretary's own initiative.
(2) A State may submit a written request to the Secretary for an advisory opinion under this paragraph. The request must include the following information:
(i) The State law for which the exception is requested;

(ii) The particular standard(s), requirement(s), or implementation specification(s) for which the exception is requested;
(iii) How health care providers, health plans, and other entities would be affected by the exception;
(iv) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets the criteria at § 160.203(b); and
(v) Any other information the Secretary may request in order to issue the advisory opinion.
(3) The requirements of paragraphs (a)(2), (a)(5)-(a)(7) of this section apply to requests for advisory opinions under this paragraph.
(4) The Secretary's decision under this paragraph will be made on the basis of the extent to which the information provided and other factors demonstrate that the criteria at § 160.203(b) are met.

(5) Advisory opinions made by the Secretary pursuant to this paragraph will be published annually in the Federal Register.

PARTS 161-163 – [RESERVED]

PART 164 – SECURITY AND PRIVACY

Subpart A – General Provisions

Sec.

Subparts B-D – [Reserved]

Subpart E – Privacy of Individually Identifiable Health Information

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

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 standards under part C of title XI of the Act and section 264 of Public Law 104-191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

Subparts B-D – [Reserved]

Subpart E – Privacy of Individually Identifiable Health Information

§ 164.502 Applicability.

In addition to the applicable provisions of part 160 of this subchapter and except as otherwise herein provided, the requirements, standards, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

§ 164.504 Definitions.

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

Business partner means, with respect to a covered entity, a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. "Business partner" includes contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. "Business partner" excludes persons who are within the covered entity's workforce, as defined in this section.

Designated record set means a group of records under the control of a covered entity from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual and which is used by the covered entity to make decisions about the individual. For purposes of this paragraph, the term "record" means any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Health care operations means the following activities undertaken by or on behalf of a covered entity that is a health plan or health care provider for the purpose of carrying out the management functions of such entity necessary for the support of treatment or payment:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines;

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

(3) Insurance rating and other insurance activities relating to the renewal of a contract for insurance, including underwriting, experience rating, and reinsurance, but only when the individuals are already enrolled in the health plan conducting such activities and the use or disclosure of protected health information relates to an existing contract of insurance (including the renewal of such a contract);

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

(5) Compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding.

Health oversight agency means an agency, person or entity, including the employees or agents thereof,

(1) That is:

(i) A public agency; or

(ii) A person or entity acting under grant of authority from or contract with a public agency; and

(2) Which performs or oversees the performance of any audit; investigation; inspection; licensure or discipline; civil, criminal, or administrative proceeding or action; or other activity necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, or of government regulatory programs for which health information is necessary for determining compliance with program standards.

Individual means the person who is the subject of protected health information, except that:

(1) "Individual" includes:

(i) With respect to adults and emancipated minors, legal representatives (such as court-appointed guardians or persons with a power of attorney), to the extent to which applicable law permits such legal representatives to exercise the person's rights in such contexts.

(ii) With respect to unemancipated minors, a parent, guardian, or person acting in loco parentis, provided that when a minor lawfully obtains a health care service without the consent of or notification to a parent, guardian, or other person acting in loco parentis, the minor shall have the exclusive right to exercise the rights of an individual under this subpart with respect to the protected health information relating to such care.

(iii) With respect to deceased persons, an executor, administrator, or other person authorized under applicable law to act on behalf of the decedent's estate.

(2) "Individual" excludes:

(i) Foreign military and diplomatic personnel and their dependents who receive health care provided by or paid for by the Department of Defense or other federal agency, or by an entity acting on its behalf, pursuant to a country-to-country agreement or federal statute; and

(ii) Overseas foreign national beneficiaries of health care provided by the Department of Defense or other federal agency, or by a non-governmental organization acting on its behalf.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and that:

(1) Is created by or received from 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) Which 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.

Law enforcement official means an officer of an 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 conduct:

(1) An investigation or official proceeding inquiring into a violation of, or failure to comply with, any law; or

(2) A criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, any law.

Payment means:

(1) The activities undertaken by or on behalf of a covered entity that is:

(i) A health plan, or by a business partner on behalf of a health plan, to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan and for provision of benefits under the health plan; or

(ii) A health care provider or health plan, or a business partner on behalf of such provider or plan, to obtain reimbursement for the provision of health care.

(2) Activities that constitute payment include:

(i) Determinations of coverage, improving methods of paying or coverage policies, adjudication or subrogation of health benefit claims;

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

(iii) Billing, claims management, and medical 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; and

(v) Utilization review activities, including precertification and preauthorization of services.

Protected health information means individually identifiable health information that is or has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form.

(1) For purposes of this definition,

(i) “Electronically transmitted” includes information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and “faxback” systems.

(ii) “Electronically maintained” means information stored by a computer or on any electronic medium from which information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

(2) “Protected health information” excludes:

(i) Individually identifiable health information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and

(ii) Individually identifiable health information of inmates of correctional facilities and detainees in detention facilities.

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 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. "Generalizable knowledge" is knowledge related to health that can be applied to populations outside of the population served by the covered entity.

Treatment means the provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and disease management) among, health care providers; the referral of a patient from one provider to another; or the coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual.

Use means the employment, application, utilization, examination, or analysis of information within an entity that holds the information.

Workforce means employees, volunteers, trainees, and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.

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

(a) Standard. A covered entity may not use or disclose an individual's protected health information, except as otherwise permitted or required by this part or as required to comply with applicable requirements of this subchapter.

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

(i) Except for research information unrelated to treatment, to carry out treatment, payment, or health care operations;

(ii) Pursuant to an authorization by the individual that complies with § 164.508; or

(iii) As permitted by and in compliance with this section or § 164.510.

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

(i) To an individual, when a request is made under § 164.514; or

(ii) When required by the Secretary under § 164.522 to investigate or determine the entity's compliance with this part.

(b)(1) Standard: minimum necessary. A covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure. This requirement does not apply to uses or disclosures that are:

(i) Made in accordance with §§ 164.508(a)(1), 164.514, or 164.522;

(ii) Required by law and permitted under § 164.510;

(iii) Required for compliance with applicable requirements of this subchapter; or

(iv) Made by a covered health care provider to a covered health plan, when the information is requested for audit and related purposes.

(2) Implementation specification: procedures. To comply with the standard in this paragraph, a covered entity must have procedures to:

(i) Identify appropriate persons within the entity to determine what information should be used or disclosed consistent with the minimum necessary standard;

(ii) Ensure that the persons identified under paragraph (b)(2)(i) of this section make the minimum necessary determinations, when required;

(iii) Within the limits of the entity's technological capabilities, provide for the making of such determinations individually.

(3) Implementation specification: reliance. When making disclosures to public officials that are permitted under § 164.510 but not required by other law, a covered entity may reasonably rely on the representations of such officials that the information requested is the minimum necessary for the stated purpose(s).

(c)(1) Standard: right of an individual to restrict uses and disclosures. (i) A covered entity that is a health care provider must permit individuals to request that uses or disclosures of protected health information for treatment, payment, or health care operations be restricted, and, if the requested restrictions are agreed to by the provider, not make uses or disclosures inconsistent with such restrictions.

(ii) This requirement does not apply:

(A) To uses or disclosures permitted under § 164.510;

(B) When the health care services provided are emergency services or the information is requested pursuant to § 164.510(k); and

(C) To disclosures to the Secretary pursuant to § 164.522.

(iii) A provider is not required to agree to a requested restriction.

(2) Implementation specifications. A covered entity must have procedures that:

(i) Provide individuals an opportunity to request a restriction on the uses and disclosures of their protected health information;

(ii) Provide that restrictions that are agreed to by the entity are reduced to writing or otherwise documented;

(iii) Enable the entity to honor such restrictions; and

(iv) Provide for the notification of others to whom such information is disclosed of such restriction.

(d)(1) Standard: use or disclosure of de-identified protected health information. The requirements of this subpart do not apply to protected health information that a covered entity has de-identified, provided, however, that:

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

(ii) If a covered entity re-identifies de-identified information, it may use or disclose such re-identified information only in accordance with this subpart.

(2) Implementation specifications. (i) A covered entity may use protected health information to create de-identified information by removing, coding, encrypting, or otherwise eliminating or concealing the information that makes such information individually identifiable.

(ii) Information is presumed not to be individually identifiable (de-identified), if:

(A) The following identifiers have been removed or otherwise concealed:

(1) Name;

(2) Address, including street address, city, county, zip code, and equivalent geocodes;

(3) Names of relatives;

(4) Name of employers;

(5) Birth date;

(6) Telephone numbers;

(7) Fax numbers;
(8) Electronic mail addresses;
(9) Social security number;
(10) Medical record number;
(11) Health plan beneficiary number;
(12) Account number;
(13) Certificate/license number;
(14) Any vehicle or other device serial number;
(15) Web Universal Resource Locator (URL);
(16) Internet Protocol (IP) address number;
(17) Finger or voice prints;
(18) Photographic images; and
(19) Any other unique identifying number, characteristic, or code that the covered entity has reason to believe may be available to an anticipated recipient of the information; and

(B) The covered entity has no reason to believe that any anticipated recipient of such information could use the information, alone or in combination with other information, to identify an individual.

(iii) Notwithstanding paragraph (d)(2)(ii) of this section, entities with appropriate statistical experience and expertise may treat information as de-identified, if they include information listed in paragraph (d)(2)(ii) of this section and they determine that the probability of identifying individuals with such identifying information retained is very low, or may remove additional information, if they have a reasonable basis to believe such additional information could be used to identify an individual.

(e)(1) Standards: business partners. (i) Except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for consultation or referral purposes, a covered entity may not disclose protected health information to a business partner without satisfactory assurance from the business partner that it will appropriately safeguard the information.

(ii) A covered entity must take reasonable steps to ensure that each business partner complies with the requirements of this subpart with respect to any task or other activity it performs on behalf of the entity, to the extent the covered entity would be required to comply with such requirements.

(2) Implementation specifications.

(i) For the purposes of this section, "satisfactory assurance" means a contract between the covered entity and the business partner to which such information is to be disclosed that establishes the permitted and required uses and disclosures of such information by the partner. The contract must provide that the business partner will:

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

(B) Not use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

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

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

(E) Ensure that any subcontractors or agents to whom it provides protected health information received from the covered entity agree to the same restrictions and conditions that apply to the business partner with respect to such information;

(F) Make available protected health information in accordance with § 164.514(a);

(G) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart;

(H) At termination of the contract, return or destroy all protected health information received from the covered entity that the business partner still maintains in any form and retain no copies of such information; and

(I) Incorporate any amendments or corrections to protected health information when notified pursuant to § 164.516(c)(3).

(ii) The contract required by paragraph (e)(2)(i) of this section must:

(A) State that the individuals whose protected health information is disclosed under the contract are intended third party beneficiaries of the contract; and

(B) Authorize the covered entity to terminate the contract, if the covered entity determines that the business partner has violated a material term of the contract required by this paragraph.

(iii) A material breach by a business partner of its obligations under the contract required by paragraph (e)(2)(i) of this section will be considered to be noncompliance of the covered entity with the applicable requirements of this subpart, if the covered entity knew or reasonably should have known of such breach and failed to take reasonable steps to cure the breach or terminate the contract.

(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 for two years following the death of such individual. This requirement does not apply to uses or disclosures for research purposes.

(g) Standard: uses and disclosures consistent with notice. Except as provided by § 164.520(g)(2), a covered entity that is required by § 164.512 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice.

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

(a) Standard. An authorization executed in accordance with this section is required in order for the covered entity to use or disclose protected health information in the following situations:

(1) Request by individual. Where the individual requests the covered entity to use or disclose the information.

(2) Request by covered entity. (i) Where the covered entity requests the individual to authorize the use or disclosure of the information. The covered entity must request and obtain an authorization from the individual for all uses and disclosures that are not:

(A) Except as provided in paragraph (a)(3) of this section, compatible with or directly related to treatment, payment, or health care operations;

(B) Covered by § 164.510;

(C) Covered by paragraph (a)(1) of this section; or

(D) Required by this subpart.

(ii) Uses and disclosures of protected health information for which individual authorization is required include, but are not limited to, the following:

(A) Use for marketing of health and non-health items and services by the covered entity;

(B) Disclosure by sale, rental, or barter;

(C) Use and disclosure to non-health related divisions of the covered entity, e.g., for use in marketing life or casualty insurance or banking services;

(D) Disclosure, prior to an individual's enrollment in a health plan, to the health plan or health care provider for making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations;

(E) Disclosure to an employer for use in employment determinations; and

(F) Use or disclosure for fundraising purposes.

(iii) A covered entity may not condition the provision to an individual of treatment or payment on the provision by the individual of a requested authorization for use or disclosure, except where the authorization is requested in connection with a clinical trial.

(iv) Except where required by law, a covered entity may not require an individual to sign an authorization for use or disclosure of protected health information for treatment, payment, or health care operations purposes.

(3) Authorization required: special cases. (i) Except as otherwise required by this subpart or permitted under § 164.510, a covered entity must obtain the authorization of the individual for the following uses and disclosures of protected health information about the individual:

(A) Use by a person other than the creator, or disclosure, of psychotherapy notes; and

(B) Use or disclosure of research information unrelated to treatment.

(ii) The requirements of paragraphs (b) through (e) of this section apply to such authorizations, as appropriate.

(iii) A covered entity may not condition treatment, enrollment in a health plan, or payment on a requirement that the individual authorize use or disclosure of psychotherapy notes relating to the individual.

(iv) For purposes of this section:

(A) 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. For purposes of this definition, "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.

(B) Research information unrelated to treatment means health information that is received or created by a covered entity in the course of conducting research, for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care, and with respect to which the covered entity has not requested payment from a third party payor.

(b) General implementation specifications for authorizations. (1) General requirements. A copy of the model form which appears in Appendix A hereto, or a document that contains the elements listed in paragraphs (c) or (d) of this section, as applicable, must be accepted by the covered entity.

(2) Defective authorizations. There is no "authorization" within the meaning of this section, if the submitted form has any of the following defects:

(i) The expiration date has passed;

(ii) The form has not been filled out completely;

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

(iv) The form lacks an element required by paragraph (c) or (d) of this section, as applicable;

(v) The information on the form is known by the covered entity to be false.

(3) Compound authorizations. Except where authorization is requested in connection with a clinical trial, an authorization for use or disclosure of protected health information for purposes other than treatment or payment may not be in the same document as an authorization for or consent to treatment or payment.

(c) Implementation specifications for authorizations requested by an individual. (1) Required elements. Before a covered entity may use or disclose protected health information of an individual pursuant to a request from the individual, it must obtain a completed authorization for use or disclosure executed by the individual that contains 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 of the covered entity, or class of entities or persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s) or entity(ies), which may include the covered entity itself, to whom the covered entity may make the requested use or disclosure;

(iv) An expiration date;

(v) Signature and date;

(vi) If the authorization is executed by a legal representative or other person authorized to act for the individual, a description of his or her authority to act or relationship to the individual;

(vii) A statement in which the individual acknowledges that he or she has the right to revoke the authorization, except to the extent that information has already been released under the authorization; and

(viii) A statement in which the individual acknowledges that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by the federal privacy law.

(2) Plain language requirement. The model form at Appendix A to this subpart may be used. If the model form at Appendix A to this subpart is not used, the authorization form must be written in plain language.

(d) Implementation specifications for authorizations for uses and disclosures requested by covered entities. (1) Required elements. Before a covered entity may use or disclose protected health information of an individual pursuant to a request that it has made, it must obtain a completed authorization for use or disclosure executed by the

individual that meets the requirements of paragraph (c) of this section and contains the following additional elements:

(i) Except where the authorization is requested for a clinical trial, a statement that it will not condition treatment or payment on the individual's providing authorization for the requested use or disclosure;

(ii) A description of the purpose(s) of the requested use or disclosure;

(iii) A statement that the individual may:

(A) Inspect or copy the protected health information to be used or disclosed as provided in § 164.514; and

(B) Refuse to sign the authorization; and

(iv) Where use or disclosure of the requested information will result in financial gain to the entity, a statement that such gain will result.

(2) Required procedures. In requesting authorization from an individual under this paragraph, a covered entity must:

(i) Have procedures designed to enable it to request only the minimum amount of protected health information necessary to accomplish the purpose for which the request is made; and

(ii) Provide the individual with a copy of the executed authorization.

(e) Revocation of authorizations. An individual may revoke an authorization to use or disclose his or her protected health information at any time, except to the extent that the covered entity has taken action in reliance thereon.

§ 164.510 Uses and disclosures for which individual authorization is not required.

A covered entity may use or disclose protected health information, for purposes other than treatment, payment, or health care operations, without the authorization of the individual, in the situations covered by this section and subject to the applicable requirements provided for by this section.

(a) General requirements. In using or disclosing protected health information under this section:

(1) Verification. A covered entity must comply with any applicable verification requirements under § 164.518(c).

(2) Health care clearinghouses. A health care clearinghouse that uses or discloses protected health information it maintains as a business partner of a covered entity may not make uses or disclosures otherwise permitted under this section that are not permitted by the terms of its contract with the covered entity under § 164.506(e).

(b) Disclosures and uses 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;

(ii) A public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect;

(iii) A person or entity other than a governmental authority that can demonstrate or demonstrates that it is acting to comply with requirements or direction of a public health authority; or

(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 and is authorized by law to be notified as necessary in the conduct of a public health intervention or investigation.

(2) Permitted use. Where the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) Disclosures and uses 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 audit, investigation, inspection, civil, criminal, or administrative proceeding or action, or other activity necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility; or

(iii) Government regulatory programs for which health information is necessary for determining compliance with program standards.

(2) Permitted use. Where a covered entity is itself a health oversight agency, the covered entity may use protected health information for health oversight activities described by paragraph (c)(1) of this section.

(d) Disclosures and uses 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; or

(ii) Where the individual is a party to the proceeding and his or her medical condition or history is at issue and the disclosure is pursuant to lawful process or otherwise authorized by law.

(2) Permitted use. Where the covered entity is itself a government agency, the covered entity may use protected health information in all cases in which it is permitted to disclose such information in the course of any judicial or administrative proceeding under paragraph (d)(1) of this section.

(3) Additional restriction. (i) Where the request for disclosure of protected health information is accompanied by a court order, the covered entity may disclose only that protected health information which the court order authorizes to be disclosed.

(ii) Where the request for disclosure of protected health information is not accompanied by a court order, the covered entity may not disclose the information requested unless a request authorized by law has been made by the agency requesting the information or by legal counsel representing a party to litigation, with a written statement certifying that the protected health information requested concerns a litigant to the proceeding and that the health condition of such litigant is at issue at such proceeding.

(e) Disclosures to coroners and medical examiners. A covered entity may disclose protected health information to a coroner or medical examiner, consistent with

applicable law, for the purposes of identifying a deceased person or determining a cause of death.

(f) Disclosures for law enforcement purposes. A covered entity may disclose protected health information to a law enforcement official if:

(1) Pursuant to process. (i) The law enforcement official is conducting or supervising a law enforcement inquiry or proceeding authorized by law and the disclosure is:

(A) Pursuant to a warrant, subpoena, or order issued by a judicial officer that documents a finding by the judicial officer;

(B) Pursuant to a grand jury subpoena; or

(C) Pursuant to an administrative request, including an administrative subpoena or summons, a civil 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 as specific and narrowly drawn as is reasonably practicable; and

(3) De-identified information could not reasonably be used.

(ii) For the purposes of this paragraph, "law enforcement inquiry or proceeding" means:

(A) An investigation or official proceeding inquiring into a violation of, or failure to comply with, law; or

(B) A criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, law.

(2) Limited information for identifying purposes. The disclosure is for the purpose of identifying a suspect, fugitive, material witness, or missing person, provided that, the covered entity may disclose only the following information:

(i) Name;

(ii) Address;

(iii) Social security number;

(iv) Date of birth;

(v) Place of birth;

(vi) Type of injury or other distinguishing characteristic; and

(vii) Date and time of treatment.

(3) Information about a victim of crime or abuse. The disclosure is of the protected health information of an individual who is or is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official represents that:

(i) Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and

(ii) Immediate law enforcement activity that depends upon obtaining such information may be necessary.

(4) Intelligence and national security activities. The disclosure is:

(i) For the conduct of lawful intelligence activities conducted pursuant to the National Security Act (50 U.S.C. 401, et seq.);

(ii) Made in connection with providing protective services to the President or other persons pursuant to 18 U.S.C. 3056; or

(iii) Made pursuant to 22 U.S.C. 2709(a)(3).

(5) Health care fraud. The covered entity believes in good faith that the information disclosed constitutes evidence of criminal conduct:

(i) That arises out of and is directly related to:

(A) The receipt of health care or payment for health care, including a fraudulent claim for health care;

(B) Qualification for or receipt of benefits, payments, or services based on a fraudulent statement or material misrepresentation of the health of the individual;

(ii) That occurred on the premises of the covered entity; or

(iii) Was witnessed by a member of the covered entity's workforce.

(5) Urgent circumstances. The disclosure is of the protected health information of an individual who is or is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official represents that:

(i) Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and

(ii) Immediate law enforcement activity that depends upon obtaining such information may be necessary.

(g) Disclosures and uses for governmental health data systems. (1) Permitted disclosures. A covered entity may disclose protected health information to a government agency, or private entity acting on behalf of a government agency, for inclusion in a governmental health data system that collects health data for analysis in support of policy, planning, regulatory, or management functions authorized by law.

(2) Permitted uses. Where a covered entity is itself a government agency that collects health data for analysis in support of policy, planning, regulatory, or management functions, the covered entity may use protected health information in all cases in which it is permitted to disclose such information for government health data systems under paragraph (g)(1) of this section.

(h) Disclosures of directory information. (1) Individuals with capacity. For individuals with the capacity to make their own health care decisions, a covered entity that is a health care provider may disclose protected health information for directory purposes, provided that, the individual has agreed to such disclosure.

(2) Incapacitated individuals. For individuals who are incapacitated, a covered entity that is a health care provider may, at its discretion and consistent with good medical practice and any prior expressions of preference of which the covered entity is aware, disclose protected health information for directory purposes.

(3) Information to be disclosed. The information that may be disclosed for directory purposes pursuant to paragraphs (h)(1) and (2) of this section, is limited to:

(i) Name of the individual;

(ii) Location of the individual in the health care provider's facility; and

(iii) Description of the individual's condition in general terms that do not communicate specific medical information about the individual.

(i) Disclosures for banking and payment processes. A covered entity may disclose, in connection with routine banking activities or payment by debit, credit, or other payment card, or other payment means, the minimum amount of protected health information necessary to complete a banking or payment activity to:

(1) Financial institutions. An entity engaged in the activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978); or

(2) Entities acting on behalf of financial institutions. An entity engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for an entity described in paragraph (i)(1) of this section.

(j) Uses and disclosures for research purposes. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that, the covered entity has obtained written documentation of the following:

(1) Waiver of authorization. A waiver, in whole or in part, of authorization for use or disclosure of protected health information that has been approved by either:

(i) An Institutional Review Board, 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, 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

(ii) A privacy board that:

(A) Has members with varying backgrounds and appropriate professional competency as necessary to review the research protocol;

(B) Includes at least one member who is not affiliated with the entity conducting the research or related to a person who is affiliated with such entity; and

(C) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(2) Date of approval. The date of approval of the waiver, in whole or in part, of authorization by an Institutional Review Board or privacy board.

(3) Criteria. The Institutional Review Board or privacy board has determined that the waiver, in whole or in part, of authorization satisfies the following criteria:

(i) The use or disclosure of protected health information involves no more than minimal risk to the subjects;

(ii) The waiver will not adversely affect the rights and welfare of the subjects;

(iii) The research could not practicably be conducted without the waiver;

(iv) Whenever appropriate, the subjects will be provided with additional pertinent information after participation;

(v) The research could not practicably be conducted without access to and use of the protected health information;

(vi) The research is of sufficient importance so as to outweigh the intrusion of the privacy of the individual whose information is subject to the disclosure;

(vii) There is an adequate plan to protect the identifiers from improper use and disclosure; and

(viii) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers.

(4) Required signature. The written documentation must be signed by the chair of, as applicable, the Institutional Review Board or the privacy board.

(k) Uses and disclosures in emergency circumstances. (1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct and based on a reasonable belief that the use or disclosure is necessary to prevent or

lessen a serious and imminent threat to the health or safety of an individual or the public, use or disclose protected health information to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

(2) Presumption of reasonable belief. A covered entity that makes a disclosure pursuant to paragraph (k)(1) of this section is presumed to have acted under a reasonable belief, if the disclosure is made in good faith based upon a credible representation by a person with apparent knowledge or authority (such as a doctor or law enforcement or other government official).

(l) Disclosures to next-of-kin. (1) Permitted disclosures. A covered entity may disclose protected health information to a person who is a next-of-kin, other family member, or close personal friend of an individual who possesses the capacity to make his or her own health care decisions, if:

(i) The individual has verbally agreed to the disclosure; or

(ii) In circumstances where such agreement cannot practicably or reasonably be obtained, only the protected health information that is directly relevant to the person's involvement in the individual's health care is disclosed, consistent with good health professional practices and ethics.

(2) Next-of-kin defined. For purposes of this paragraph, "next-of-kin" is defined as defined under applicable law.

(m) Uses and disclosures for specialized classes. (1) Military purposes. A covered entity that is a health care provider or health plan providing health care to individuals who are Armed Forces personnel may use and disclose protected health information for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, where the appropriate military authority has published by notice in the Federal Register the following information:

(i) Appropriate military command authorities;

(ii) The circumstances for which use or disclosure without individual authorization would be required; and

(iii) Activities for which such use or disclosure would occur in order to assure proper execution of the military mission.

(2) Department of Veterans Affairs. The Department of Veterans Affairs may use and disclose protected health information among components of the Department that determine eligibility for or entitlement to, or that provide, benefits under laws administered by the Secretary of Veterans Affairs.

(3) Intelligence community. A covered entity may disclose protected health information of an individual who is an employee of the intelligence community, as defined in Section 4 of the National Security Act, 50 U.S.C. 401a, and his or her dependents, if such dependents are being considered for posting abroad, to intelligence community agencies, where authorized by law.

(4) Department of State. The Department of State may use protected health information about the following individuals for the following purposes:

(i) As to applicants to the Foreign Service, for medical clearance determinations about physical fitness to serve in the Foreign Service on a worldwide basis, including about medical and mental conditions limiting assignability abroad; determinations of conformance to occupational physical standards, where applicable; and determinations of suitability.

(ii) As to members of the Foreign Service and other United States Government employees assigned to serve abroad under Chief of Mission authority, for medical clearance determinations for assignment to posts abroad, including medical and mental conditions limiting such assignment; determinations of conformance to occupational physical standards, where applicable; determinations about continued fitness for duty, suitability, and continuation of service at post (including decisions on curtailment); separation medical examinations; and determinations of eligibility of members of the Foreign Service for disability retirement (whether on application of the employee or the Secretary of State).

(iii) As to eligible family members of Foreign Service or other United States Government employees, for medical clearance determinations as described in paragraph (m)(4)(ii) of this section to permit eligible family members to accompany employees to posts abroad on Government orders; determinations regarding family members remaining at post; and separation medical examinations.

(n) Uses and disclosures otherwise required by law. A covered entity may use or disclose protected health information where such use or disclosure is required by law and the use or disclosure meets all relevant requirements of such law. This paragraph does not apply to uses or disclosures that are covered by paragraphs (b) through (m) of this section.

§ 164.512 Notice to individuals of information practices.

(a) Standard. An individual has a right to adequate notice of the policies and procedures of a covered entity that is a health plan or a health care provider with respect to protected health information.

(b) Standard for notice procedures. A covered entity that is a health plan or health care provider must have procedures that provide adequate notice to individuals of their rights and the procedures for exercising their rights under this subpart with respect to protected health information about them.

(c) General implementation specification. A covered entity that has and follows procedures that meet the requirements of this section will be presumed to have provided adequate notice under this section.

(d) Implementation specifications: content of notice. (1) Required elements. Notices required to be provided under this section must include in plain language a statement of each of the following elements:

(i) Uses and disclosures. The uses and disclosures, and the entity's policies and procedures with respect to such uses and disclosures, must be described in sufficient detail to put the individual on notice of the uses and disclosures expected to be made of his or her protected health information. Such statement must:

(A) Describe the uses and disclosures that will be made without individual authorization; and

(B) Distinguish between those uses and disclosures the entity makes that are required by law and those that are permitted but not required by law.

(ii) Required statements. State that:

(A) Other uses and disclosures will be made only with the individual's authorization and that such authorization may be revoked;

(B) An individual may request that certain uses and disclosures of his or her protected health information be restricted, and the covered entity is not required to agree to such a request;

(C) An individual has the right to request, and a description of the procedures for exercising, the following with respect to his or her protected health information:

(1) Inspection and copying;

(2) Amendment or correction; and

(3) An accounting of the disclosures of such information by the covered entity;

(D) The covered entity is required by law to protect the privacy of its individually identifiable health information, provide a notice of its policies and procedures with respect to such information, and abide by the terms of the notice currently in effect;

(E) The entity may change its policies and procedures relating to protected health information at any time, with a description of how individuals will be informed of material changes; and

(F) Individuals may complain to the covered entity and to the Secretary if they believe that their privacy rights have been violated.

(iii) Contact. The name and telephone number of a contact person or office required by § 164.518(a)(2).

(iv) Date. The date the version of the notice was produced.

(2) Revisions. A covered health plan or health care provider may change its policies or procedures required by this subpart at any time. When a covered health plan or health care provider materially revises its policies and procedures, it must update its notice as provided for by § 164.520(g).

(e) Implementation specifications: provision of notice. A covered entity must make the notice required by this section available:

(1) General requirement. On request; and

(2) Specific requirements. As follows:

(i) Health plans. Health plans must provide a copy of the notice to an individual covered by the plan:

(A) As of the date on which the health plan is required to be in compliance with this subpart;

(B) After the date described in paragraph (e)(2)(i)(A) of this section, at enrollment;

(C) After enrollment, within 60 days of a material revision to the content of the notice; and

(D) No less frequently than once every three years.

(ii) Health care providers. A health care provider must:

(A) During the one year period following the date by which the provider is required to come into compliance with this subpart, provide a copy to individuals currently served by the provider at the first service delivery to such individuals during such period, provided that, where service is not provided through a face-to-face contact, the provider must provide the notice in an appropriate manner within a reasonable period of time following first service delivery;

(B) After the one year period provided for by paragraph (e)(2)(ii)(A) of this section, provide a copy to individuals served by the provider at the first service delivery to such individuals, provided that, where service is not provided through a face-to-face

contact, the provider must provide the notice in an appropriate manner within a reasonable period of time following first service delivery; and

(C) Post a copy of the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the provider to be able to read the notice. Any revision to the notice must be posted promptly.

§ 164.514 Access of individuals to protected health information

(a) Standard: right of access. An individual has a right of access to, which includes a right to inspect and obtain a copy of, his or her protected health information in designated record sets of a covered entity that is a health plan or a health care provider, including such information in a business partner's designated record set that is not a duplicate of the information held by the provider or plan, for so long as the information is maintained.

(b) Standard: denial of access to protected health information. (1) Grounds. Except where the protected health information to which access is requested is subject to 5 U.S.C. 552a, a covered entity may deny a request for access under paragraph (a) of this section where:

(i) A licensed health care professional has determined that, in the exercise of reasonable professional judgment, the inspection and copying requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The information is about another person (other than a health care provider) and a licensed health care professional has determined that the inspection and copying requested is reasonably likely to cause substantial harm to such other person;

(iii) The information was obtained under a promise of confidentiality from someone other than a health care provider and such access would be likely to reveal the source of the information;

(iv) The information was obtained by a covered entity that is a health care provider in the course of a clinical trial, the individual has agreed to the denial of access when consenting to participate in the trial (if the individual's consent to participate was obtained), and the clinical trial is in progress; or

(v) The information was compiled in reasonable anticipation of, or for use in, a legal proceeding.

(2) Other information available. Where a denial of protected health information is made pursuant to paragraph (b)(1) of this section, the covered entity must make any other protected health information requested available to the individual to the extent possible consistent with the denial.

(c) Standard: procedures to protect rights of access. A covered entity that is a health plan or a health care provider must have procedures that enable individuals to exercise their rights under paragraph (a) of this section.

(d) Implementation specifications: access to protected health information. The procedures required by paragraph (c) of this section must:

(1) Means of request. Provide a means by which an individual can request inspection or a copy of protected health information about him or her.

(2) Time limit. Provide for taking action on such requests as soon as possible but not later than 30 days following receipt of the request.

(3) Request accepted. Where the request is accepted, provide:

(i) For notification of the individual of the decision and of any steps necessary to fulfill the request;

(ii) The information requested in the form or format requested, if it is readily producible in such form or format;

(iii) For facilitating the process of inspection and copying; and

(iv) For a reasonable, cost-based fee for copying health information provided pursuant to this paragraph, if deemed desirable by the entity.

(4) Request denied. Where the request is denied in whole or in part, provide the individual with a written statement in plain language of:

(i) The basis for the denial; and

(ii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518(d)(2) or to the Secretary pursuant to the procedures established in § 164.522(b). The description must include:

(A) The name and telephone number of the contact person or office required by § 164.518(a)(2); and

(B) Information relevant to filing a complaint with the Secretary under § 164.522(b).

§164.515 Accounting for disclosures of protected health information.

(a) Standard: right to an accounting of disclosures of protected health information. An individual has a right to receive an accounting of all disclosures of protected health information made by a covered entity as long as such information is maintained by the entity, except for disclosures:

(1) For treatment, payment and health care operations; and

(2) To health oversight or law enforcement agencies, if the health oversight or law enforcement agency has provided a written request stating that the exclusion is necessary because disclosure would be reasonably likely to impede the agency's activities and specifying the time for which such exclusion is required.

(b) Standard: procedures for accounting. A covered entity must have procedures to give individuals an accurate accounting of disclosures for which an accounting is required by paragraph (a) of this section.

(c) Implementation specifications: accounting procedures. The procedures required by paragraph (b) of this section must:

(1) Provide for an accounting of the following:

(i) The date of each disclosure;

(ii) The name and address of the organization or person who received the protected health information;

(iii) A brief description of the information disclosed;

(iv) For disclosures other than those made at the request of the individual, the purpose for which the information was disclosed; and

(v) Provision of copies of all requests for disclosure.

(2) Provide the accounting to the individual as soon as possible, but no later than 30 days of receipt of the request therefor.

(3) Provide for a means of accounting for as long as the entity maintains the protected health information.

(4) Provide for a means of requiring business partners to provide such an accounting upon request of the covered entity.

§ 164.516 Amendment and correction.

(a) Standard: right to request amendment or correction. (1) Right to request. An individual has the right to request a covered entity that is a health plan or health care provider to amend or correct protected health information about him or her in designated record sets of the covered entity for as long as the covered entity maintains the information.

(2) Grounds for denial of request. A covered entity may deny a request for amendment or correction of the individual's protected health information, if it determines that the information that is the subject of the request:

(i) Was not created by the covered entity;

(ii) Would not be available for inspection and copying under § 164.514; or

(iii) Is accurate and complete.

(b) Standard: amendment and correction procedures. A covered entity that is a health plan or health care provider must have procedures to enable individuals to request amendment or correction, to determine whether the requests should be granted or denied, and to disseminate amendments or corrections to its business partners and others to whom erroneous information has been disclosed.

(c) Implementation specifications: procedures. The procedures required by paragraph (b) of this section must provide that the covered entity will:

(1) Means of request. Provide a means by which an individual can request amendment or correction of his or her protected health information.

(2) Time limit. Take action on such request within 60 days of receipt of the request;

(3) Request accepted. Where the request is accepted in whole or in part:

(i) As otherwise required by this part, make the appropriate amendments or corrections;

(ii) As otherwise required by this part, identify the challenged entries as amended or corrected and indicate their location;

(iii) Make reasonable efforts to notify:

(A) Persons, organizations, or other entities the individual identifies as needing to be notified; and

(B) Persons, organizations, or other entities, including business partners, who the covered entity knows have received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual; and

(iv) Notify the individual of the decision to correct or amend the information.

(4) Request denied. Where the request is denied in whole or in part:

(i) Provide the individual with a written statement in plain language of:

(A) The basis for the denial;

(B) A description of how the individual may file a written statement of disagreement with the denial; and

(C) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518(d) or to the Secretary pursuant to the procedures established in § 164.522(b). The description must include:

(1) The name and telephone number of the contact person or office required by § 164.518(a)(2); and

(2) Information relevant to filing a complaint with the Secretary under § 164.522(b).

(ii) The procedures of the covered entity must:

(A) Permit the individual to file a statement of the individual's disagreement with the denial and the basis of such disagreement.

(B) Provide for inclusion of the covered entity's statement of denial and the individual's statement of disagreement with any subsequent disclosure of the information to which the disagreement relates, provided, however, that the covered entity may establish a limit to the length of the statement of disagreement, and may summarize the statement of disagreement if necessary.

(C) Permit the covered entity to provide a rebuttal to the statement of disagreement in subsequent disclosures under paragraph (c)(4)(ii)(B) of this section.

(d) Standard: effectuating a notice of amendment or correction. Any covered entity that receives a notice of amendment or correction must have procedures in place to make the amendment or correction in any of its designated record sets and to notify its business partners, as appropriate, of necessary amendments or corrections of protected health information.

(e) Implementation specification: effectuating a notice of amendment or correction. The procedures required by paragraph (d) of this section must specify the process for correction or amendment of information in all appropriate designated record sets maintained by the covered entity and its business partners.

§ 164.518 Administrative requirements.

Except as otherwise provided, a covered entity must meet the requirements of this section.

(a) Designated privacy official: standard. (1) Responsibilities of designated privacy official. A covered entity must designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the entity.

(2) Contact person or office. 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 § 164.512. If a covered entity designates a contact person, it may designate the privacy official as the contact person.

(b) Training. (1) Standard. All members of the covered entity's workforce who, by virtue of their positions, are likely to obtain access to protected health information must receive training on the entity's policies and procedures required by this subpart that are relevant to carrying out their function within the entity.

(2) Implementation specification. A covered entity must train all members of its workforce who, by virtue of their positions, are likely to obtain access to protected health information. Such training must meet the following requirements:

(i) The training must occur:

(A) For members of the covered entity's workforce as of the date on which this subpart becomes applicable to such entity, by such date; and

(B) For persons joining the covered entity's workforce after the date in paragraph (b)(2)(i)(A) of this section, within a reasonable period after the person joins the workforce.

(ii) The covered entity must require members of its workforce trained as required by this section to sign, upon completing training, a certification. The certification must state:

(A) The date of training; and

(B) That the person completing the training will honor all of the entity's policies and procedures required by this subpart.

(iii) The covered entity must require members of its workforce trained as required by this section to sign, at least once every three years, a statement certifying that the person will honor all of the entity's policies and procedures required by this subpart.

(iv) The covered entity must provide all members of its workforce with access to protected health information within the entity with further training, as relevant to their function within the entity, whenever the entity materially changes its privacy policies or procedures.

(c) Safeguards. (1) Standard. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) Implementation specification: verification procedures. A covered entity must have administrative, technical, and physical procedures in place to protect the privacy of protected health information. Such procedures must include adequate procedures for verification of the identity and/or authority, as required by this subpart, of persons requesting such information, where such identity or authority is not known to the entity, as follows:

(i) The covered entity must use procedures that are reasonably likely to establish that the individual or person making the request has the appropriate identity for the use or disclosure requested, except for uses and disclosures that are:

(A) Permitted by this subpart and made on a routine basis to persons or other entities with which the covered entity interacts in the normal course of business or otherwise known to the covered entity; or

(B) Covered by paragraphs (c)(2)(ii), (iii), or (iv) of this section.

(ii) When the request for information is made by a government agency under § 164.510 (b), § 164.510(c), § 164.510(e), § 164.510(f), § 164.510(g), § 164.510(m), § 164.510(n), or § 164.522, and the identity and/or authority are not known to the covered entity, the covered entity may not disclose such information without reasonable evidence of identity and/or authority to obtain the information.

(A) For purposes of this paragraph, "reasonable evidence of identity" means:

(1) A written request on the agency's letterhead;

(2) Presentation of an agency identification badge or official credentials; or

(3) Similar proof of government status.

(B) For purposes of this paragraph, "reasonable evidence of authority" means:

(1) A written statement of the legal authority under which the information is requested; a request for disclosure made by official legal process issued by a grand jury or a judicial or administrative body is presumed to constitute reasonable legal authority; or

(2) Where the request is made orally, an oral statement of such authority.

(iii) When the request for information is made by a person or entity acting on behalf of a government agency under § 164.510(b), § 164.510(c), § 164.510(g), or §

164.510(n), and the identity and/or authority are not known to the covered entity, the covered entity may not disclose such information without reasonable evidence of identity and/or authority to obtain the information.

(A) For the purposes of this paragraph, "reasonable evidence of identity" means:

(1) A written statement from the government agency, on the agency's letterhead, that the person or entity is acting under the agency's authority; or

(2) Other evidence or documentation, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person or entity is acting on behalf of or under the agency's authority.

(B) For the purposes of this paragraph, "reasonable evidence of authority" means a statement that complies with paragraph (c)(ii)(B) of this section.

(iv) For uses and disclosures under § 164.510(d), § 164.510(h), or § 164.510(j), compliance with the applicable requirements of those sections constitutes adequate verification under this section.

(v) (A) A covered entity may reasonably rely on evidence of identity and legal authority that meets the requirements of this paragraph.

(B) Where presentation of particular documentation or statements are required by this subpart as a condition of disclosure, a covered entity may reasonably rely on documentation or statements that on their face meet the applicable requirements.

(3) Implementation specification: other safeguards. A covered entity must have safeguards to ensure that information is not used in violation of the requirements of this subpart or by members of its workforce or components of the entity or employees and other persons associated with, or components of, its business partners who are not authorized to access the information.

(4) Implementation specification: disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart where a member of its workforce or an employee or other person associated with a business partner discloses protected health information that such member or other person believes is evidence of a violation of law to:

(i) The law enforcement official or oversight agency authorized to enforce such law; or

(ii) An attorney, for the purpose of determining whether a violation of law has occurred or assessing what remedies or actions at law may be available to the employee.

(d) Complaints to the covered entity. (1) Standard. A covered entity that is a health plan or health care provider must provide a process whereby individuals may make complaints concerning the entity's compliance with the requirements established by this subpart.

(2) Implementation specifications. A covered entity that is a health plan or health care provider must develop and implement procedures under which an individual may file a complaint alleging that the covered entity failed to comply with one or more requirements of this subpart. Such procedures must provide for:

(i) The identification of the contact person or office required by paragraph (a)(2) of this section; and

(ii) Maintenance by the covered entity of a record of all complaints and their disposition, if any.

(e) Sanctions: standard. A covered entity must develop and apply when appropriate sanctions against members of its workforce who fail to comply with the policies and procedures of the covered entity or the requirements of this subpart in connection with protected health information held by the covered entity or its business partners.

(f) Duty to mitigate: standard. A covered entity must have procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information in violation of this subpart.

§164.520 Documentation of policies and procedures.

(a) Standard. A covered entity must adequately document its compliance with the applicable requirements of this subpart.

(b) Implementation specification: general. A covered entity must document its policies and procedures for complying with the applicable requirements of this subpart. Such documentation must include, but is not limited to, documentation that meets the requirements of paragraphs (c) through (g) of this section.

(c) Implementation specification: uses and disclosures. With respect to uses by the covered entity or its business partners of protected health information, a covered entity must document its policies and procedures regarding:

(1) Uses and disclosures of such information, including:

(i) Uses and disclosures with authorization, including for revocation of authorizations; and

(ii) Uses and disclosures without authorization, including:

(A) For treatment, payment, and health care operations;

(B) For disclosures to business partners, including monitoring and mitigation; and

(C) For uses and disclosures pursuant to § 164.510.

(2) For implementation of the minimum necessary requirement of § 164.506(b).

(3) For implementation of the right to request a restriction under § 164.506(c), including:

(A) Who, if anyone, in the covered entity is authorized to agree to such a request; and

(B) How restrictions agreed to are implemented.

(4) For creation of de-identified information in accordance with § 164.506(d).

(d) Implementation specification: individual rights. A covered entity must document its policies and procedures under §§ 164.512, 164.514, 164.515, and 164.516, as applicable, including:

(1) How notices will be disseminated in accordance with § 164.512;

(2) Designated record sets to which access will be granted under § 164.514;

(3) Grounds for denying requests for access under § 164.514;

(4) Copying fees, if any;

(5) Procedures for providing accounting pursuant to § 164.515;

(6) Procedures for accepting or denying requests for amendment or correction under § 164.516;

(7) How other entities will be notified of amendments or corrections accepted under § 164.516; and

(8) Identification of persons responsible for making decisions or otherwise taking action, including serving as a contact person, under §§ 164.512, 164.514, 164.515, and 164.516.

(e) Implementation specification: administrative requirements. A covered entity must provide documentation of its procedures for complying with § 164.518, including:

(1) Identification of the persons or offices required by § 164.518(a) and their duties;

(2) Training provided as required by § 164.518(b);

(3) How access to protected health information is regulated by the covered entity and its business partners, including safeguards required by § 164.518(c);

(4) For a covered entity that is a health plan or health care provider, for receiving complaints under § 164.518(d);

(5) Sanctions, and the application thereof, required by § 164.518(e); and

(6) Procedures for mitigation under § 164.518(f).

(f) Implementation specification: specific documentation required. A covered entity must retain documentation of the following for six years from when the documentation is created, unless a longer period applies under this subpart:

(1) Restrictions agreed to pursuant to § 164.506(c);

(2) Contracts pursuant to § 164.506(e);

(3) Authorization forms used pursuant to § 164.508;

(4) Samples of all notices issued pursuant to § 164.512;

(5) Written statements required by § 164.514;

(6) The accounting required by § 164.515;

(7) Documents relating to denials of requests for amendment and correction pursuant to § 164.516;

(8) Certifications under § 164.518(b); and

(9) Complaints received and any responses thereto pursuant to § 164.518(d).

(g) Implementation specification: change in policy or procedure. (1) Except as provided in paragraph (g)(2) of this section, a covered entity may not implement a change to a policy or procedure required or permitted under this subpart until it has made the appropriate changes to the documentation required by this section and the notice required by § 164.512.

(2) Where the covered entity determines that a compelling reason exists to make a use or disclosure or take another action permitted under this subpart that its notice and policies and procedures do not permit, it may make the use or disclosure or take the other action if:

(1) It documents the reasons supporting the use, disclosure, or other action; and

(2) Within 30 days of the use, disclosure, or other action, changes its notice, policies and procedures to permit such use, disclosure, or other action.

§ 164.522 Compliance and enforcement.

(a) Principles for achieving compliance.

(1) Cooperation. The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the requirements established under this subpart.

(2) Assistance. The Secretary may provide technical assistance to covered entities to help them comply voluntarily with this subpart.

(b) Individual complaints to the Secretary. An individual who believes that a covered entity is not complying with the requirements of this subpart may file a complaint with the Secretary, provided that, where the complaint relates to the alleged failure of a covered entity to amend or correct protected health information pursuant to § 164.516, the Secretary may determine whether the covered entity has followed procedures that comply with § 164.516, but will not determine whether the information involved is accurate, complete, or whether errors or omissions might have an adverse effect on the individual.

(1) Requirements for filing complaints. Complaints under this section must meet the following requirements:

(i) A complaint must be filed in writing, either on paper or electronically.

(ii) A complaint should name the entity that is the subject of the complaint and describe in detail the acts or omissions believed to be in violation of the requirements of this subpart.

(iii) The Secretary may prescribe additional requirements for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

(2) Investigation. The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, practices, and procedures of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

(c) Compliance reviews. The Secretary may conduct compliance reviews to determine whether covered entities are complying with this subpart.

(d) Responsibilities of covered entities.

(1) Provide records and compliance reports. A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the requirements of this subpart.

(2) Cooperate with periodic compliance reviews. The covered entity shall cooperate with the Secretary if the Secretary undertakes a review of the policies, procedures, and practices of a covered entity to determine whether it is complying with this subpart.

(3) Permit access to information. A covered entity must permit access by the Secretary during normal business hours to its books, records, accounts, and other sources of information, including protected health information, and its facilities, that are pertinent to ascertaining compliance with this subpart. Where any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information. Protected health information obtained in connection with a compliance review or investigation under this subpart will not be disclosed by the Secretary, except where necessary to enable the Secretary to ascertain compliance with this subpart, in formal enforcement proceedings, or where otherwise required by law.

(4) Refrain from intimidating or retaliatory acts. A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the filing of a complaint under this section, for testifying, assisting,

participating in any manner in an investigation, compliance review, proceeding or hearing under this Act, or opposing any act or practice made unlawful by this subpart.

(e) Secretarial action regarding complaints and compliance reviews.

(1) Resolution where noncompliance is indicated. (i) If an investigation pursuant to paragraph (b)(2) of this section or a compliance review pursuant to paragraph (c) of this section indicates a failure to comply, the Secretary will so inform the covered entity and, where the matter arose from a complaint, the individual, and resolve the matter by informal means whenever possible.

(ii) If the Secretary determines that the matter cannot be resolved by informal means, the Secretary may issue written findings documenting the non-compliance to the covered entity and, where the matter arose from a complaint, to the complainant. The Secretary may use such findings as a basis for initiating action under section 1176 of the Act or initiating a criminal referral under section 1177.

(2) Resolution where no violation is found. If an investigation or compliance review does not warrant action pursuant to paragraph (e)(1) of this section, the Secretary will so inform the covered entity and, where the matter arose from a complaint, the individual in writing.

§ 164.524 Effective date.

A covered entity must be in compliance with this subpart not later than 24 months following the effective date of this rule, except that a covered entity that is a small health plan must be in compliance with this subpart not later than 36 months following the effective date of the rule.