

HIPAA Privacy WorkGroups™

The innovative approach to self-implementation

HIPAA Overview

Introduction to
Administrative
Simplification

HIPAA Privacy
Regulations:
In-depth Summary

Gregory D. Frost

ROEDEL PARSONS KOCH FROST BALHOFF & MCCOLLISTER

Baton Rouge, Louisiana

GFrost@RoedelParsons.com

PUBLIC LAW 104-191

AUG. 21, 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104-191
104th Congress

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

* * *

TITLE I--HEALTH CARE ACCESS, PORTABILITY, AND RENEWABILITY

* * *

TITLE II--PREVENTING HEALTH CARE FRAUD AND ABUSE; ADMINISTRATIVE SIMPLIFICATION; MEDICAL LIABILITY REFORM

* * *

Subtitle F--Administrative Simplification

- Sec. 261. Purpose.
- Sec. 262. Administrative simplification.

Part C--Administrative Simplification

- Sec. 1171. Definitions.
- Sec. 1172. General requirements for adoption of standards.
- Sec. 1173. Standards for information transactions and data elements.
- Sec. 1174. Timetables for adoption of standards.
- Sec. 1175. Requirements.
- Sec. 1176. General penalty for failure to comply with requirements and standards.

HIPAA Overview

- Sec. 1177. Wrongful disclosure of individually identifiable health information.
- Sec. 1178. Effect on State law.
- Sec. 1179. Processing payment transactions..

* * *

Sec. 263. Changes in membership and duties of National Committee on Vital and Health Statistics.

Sec. 264. Recommendations with respect to privacy of certain health information.

* * *

Subtitle F--Administrative Simplification

SEC. 261. PURPOSE.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.

SEC. 262. ADMINISTRATIVE SIMPLIFICATION.

(a) IN GENERAL.--Title XI (42 U.S.C. 1301 et seq.) is amended by adding at the end the following:

PART C--ADMINISTRATIVE SIMPLIFICATION

SEC. 1171. Definitions. For purposes of this part:

(1) **CODE SET.**--The term 'code set' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

(2) **HEALTH CARE CLEARINGHOUSE.**--The term 'health care clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

(3) **HEALTH CARE PROVIDER.**--The term 'health care provider' includes a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)), and any other person furnishing health care services or supplies.

HIPAA Overview

(4) HEALTH INFORMATION.--The term 'health information' means any information, whether oral or recorded in any form or medium, that--

- (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

(5) HEALTH PLAN.--The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act). Such term includes the following, and any combination thereof:

(A) A group health plan (as defined in section 2791(a) of the Public Health Service Act), but only if the plan—

- (i) has 50 or more participants (as defined in section 3(7) of the Employee Retirement Income Security Act of 1974); or
- (ii) is administered by an entity other than the employer who established and maintains the plan.

(B) A health insurance issuer (as defined in section 2791(b) of the Public Health Service Act).

(C) A health maintenance organization (as defined in section 2791(b) of the Public Health Service Act).

(D) Part A or part B of the Medicare program under title XVIII.

(E) The medicaid program under title XIX.

(F) A Medicare supplemental policy (as defined in section 1882(g)(1)).

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

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

(I) The health care program for active military personnel under title 10, United States Code.

HIPAA Overview

(J) The veterans health care program under chapter 17 of title 38, United States Code.

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

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

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

(6) **INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.**--The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that—

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

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

(i) identifies the individual; or

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

(7) **STANDARD.**--The term 'standard', when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174.

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

HIPAA Overview

GENERAL REQUIREMENTS FOR ADOPTION OF STANDARDS

SEC. 1172. General Requirements for adoption of standards

(a) **APPLICABILITY.**--Any standard adopted under this part shall apply, in whole or in part, to the following persons:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).

(b) **REDUCTION OF COSTS.**--Any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.

(c) **ROLE OF STANDARD SETTING ORGANIZATIONS.**—

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

(2) **SPECIAL RULES.**--

(A) **DIFFERENT STANDARDS.**--The Secretary may adopt a standard that is different from any standard developed, adopted, or modified by a standard setting organization, if--

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

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

(B) **NO STANDARD BY STANDARD SETTING ORGANIZATION.**--If no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt under this part—

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

(ii) subsection (f) shall apply.

HIPAA Overview

(3) CONSULTATION REQUIREMENT.—

(A) IN GENERAL.--A standard may not be adopted under this part unless—

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

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

(B) ORGANIZATIONS DESCRIBED.--The organizations referred to in subparagraph (A) are the following:

(i) The National Uniform Billing Committee.

(ii) The National Uniform Claim Committee.

(iii) The Workgroup for Electronic Data Interchange.

(iv) The American Dental Association.

(d) IMPLEMENTATION SPECIFICATIONS.--The Secretary shall establish specifications for implementing each of the standards adopted under this part.

(e) PROTECTION OF TRADE SECRETS.--Except as otherwise required by law, a standard adopted under this part shall not require disclosure of trade secrets or confidential commercial information by a person required to comply with this part.

(f) ASSISTANCE TO THE SECRETARY.--In complying with the requirements of this part, the Secretary shall rely on the recommendations of the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)), and shall consult with appropriate Federal and State agencies and private organizations. The Secretary shall publish in the Federal Register any recommendation of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.

(g) APPLICATION TO MODIFICATIONS OF STANDARDS.--This section shall apply to a modification to a standard (including an addition to a standard) adopted under section 1174(b) in the same manner as it applies to an initial standard adopted under section 1174(a).

HIPAA Overview

SEC. 1173. Standards for information transactions and data elements

(a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.—

(1) IN GENERAL.--The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for—

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

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

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

(A) Health claims or equivalent encounter information.

(B) Health claims attachments.

(C) Enrollment and disenrollment in a health plan.

(D) Eligibility for a health plan.

(E) Health care payment and remittance advice.

(F) Health plan premium payments.

(G) First report of injury.

(H) Health claim status.

(I) Referral certification and authorization.

(3) ACCOMMODATION OF SPECIFIC PROVIDERS.--The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

(b) UNIQUE HEALTH IDENTIFIERS.—

(1) IN GENERAL.--The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan

HIPAA Overview

and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

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

(c) CODE SETS.—

(1) IN GENERAL.--The Secretary shall adopt standards that—

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

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

(2) DISTRIBUTION.--The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

(d) SECURITY STANDARDS FOR HEALTH INFORMATION.—

(1) SECURITY STANDARDS.--The Secretary shall adopt security standards that—

(A) take into account—

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

(ii) the costs of security measures;

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

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

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

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

HIPAA Overview

(2) SAFEGUARDS.--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—

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

(B) to protect against any reasonably anticipated—

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

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

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

(e) ELECTRONIC SIGNATURE.—

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

(2) EFFECT OF COMPLIANCE.--Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

(f) TRANSFER OF INFORMATION AMONG HEALTH PLANS.--The Secretary shall adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan.

SEC. 1174. Timetables for adoption of standards

(a) INITIAL STANDARDS.--The Secretary shall carry out section 1173 not later than 18 months after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, except that standards relating to claims attachments shall be adopted not later than 30 months after such date.

(b) ADDITIONS AND MODIFICATIONS TO STANDARDS.—

(1) IN GENERAL.--Except as provided in paragraph (2), the Secretary shall review the standards adopted under section 1173, and shall adopt modifications to the standards (including additions to the standards), as determined appropriate, but not more frequently

HIPAA Overview

than once every 12 months. Any addition or modification to a standard shall be completed in a manner which minimizes the disruption and cost of compliance.

(2) SPECIAL RULES.—

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

(B) ADDITIONS AND MODIFICATIONS TO CODE SETS.—

(i) IN GENERAL.--The Secretary shall ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets.

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

SEC. 1175. Requirements

a) CONDUCT OF TRANSACTIONS BY PLANS.—

(1) IN GENERAL.--If a person desires to conduct a transaction referred to in section 1173(a)(1) with a health plan as a standard transaction—

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

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

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

HIPAA Overview

(2) **SATISFACTION OF REQUIREMENTS.**--A health plan may satisfy the requirements under paragraph (1) by—

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

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

(3) **TIMETABLE FOR COMPLIANCE.**--Paragraph (1) shall not be construed to require a health plan to comply with any standard, implementation specification, or modification to a standard or specification adopted or established by the Secretary under sections 1172 through 1174 at any time prior to the date on which the plan is required to comply with the standard or specification under subsection (b).

(b) **COMPLIANCE WITH STANDARDS.**—

(1) **INITIAL COMPLIANCE.**—

(A) **IN GENERAL.**--Not later than 24 months after the date on which an initial standard or implementation specification is adopted or established under sections 1172 and 1173, each person to whom the standard or implementation specification applies shall comply with the standard or specification.

(B) **SPECIAL RULE FOR SMALL HEALTH PLANS.**--In the case of a small health plan, paragraph (1) shall be applied by substituting '36 months' for '24 months'. For purposes of this subsection, the Secretary shall determine the plans that qualify as small health plans.

(2) **COMPLIANCE WITH MODIFIED STANDARDS.**--If the Secretary adopts a modification to a standard or implementation specification under this part, each person to whom the standard or implementation specification applies shall comply with the modified standard or implementation specification at such time as the Secretary determines appropriate, taking into account the time needed to comply due to the nature and extent of the modification. The time determined appropriate under the preceding sentence may not be earlier than the last day of the 180-day period beginning on the date such modification is adopted. The Secretary may extend the time for compliance for small health plans, if the Secretary determines that such extension is appropriate.

(3) **CONSTRUCTION.**--Nothing in this subsection shall be construed to prohibit any person from complying with a standard or specification by—

HIPAA Overview

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

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

SEC. 1176. General penalty for failure to comply with requirements and standards

(a) GENERAL PENALTY.—

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

(2) PROCEDURES.--The provisions of section 1128A (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1128A.

(b) LIMITATIONS.—

(1) OFFENSES OTHERWISE PUNISHABLE.--A penalty may not be imposed under subsection (a) with respect to an act if the act constitutes an offense punishable under section 1177.

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

(3) FAILURES DUE TO REASONABLE CAUSE.—

(A) IN GENERAL.--Except as provided in subparagraph (B), a penalty may not be imposed under subsection (a) if--

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

(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising

HIPAA Overview

reasonable diligence would have known, that the failure to comply occurred.

(B) EXTENSION OF PERIOD.—

(i) NO PENALTY.--The period referred to in subparagraph (A)(ii) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure to comply.

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

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

SEC. 1177. Wrongful disclosure of individually identifiable health information

(a) OFFENSE.--A person who knowingly and in violation of this part--

- (1) uses or causes to be used a unique health identifier;
- (2) obtains individually identifiable health information relating to an individual; or
- (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).

(b) PENALTIES.--A person described in subsection (a) shall—

- (1) be fined not more than \$50,000, imprisoned not more than 1 year, or both;
- (2) if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and
- (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.

HIPAA Overview

EFFECT ON STATE LAW

SEC. 1178. Effect on state law

(a) GENERAL EFFECT.—

(1) GENERAL RULE.--Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

(2) EXCEPTIONS.--A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall not supersede a contrary provision of State law, if the provision of State law—

(A) is a provision the Secretary determines—

(i) is necessary—

(I) to prevent fraud and abuse;

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

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

(IV) for other purposes; or

(ii) addresses controlled substances; or

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

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

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

SEC. 1179. Processing payment transactions by financial institutions

To the extent that an entity is engaged in activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

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

(2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph (1)—

(A) for transferring receivables;

(B) for auditing;

(C) in connection with—

(i) a customer dispute; or

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

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

(E) for reporting to consumer reporting agencies; or

(F) for complying with—

(i) a civil or criminal subpoena; or

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

* * *

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(a) **IN GENERAL.**--Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) **SUBJECTS FOR RECOMMENDATIONS.**--The recommendations under subsection (a) shall address at least the following:

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

(c) **REGULATIONS.**—

(1) **IN GENERAL.**--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).

(2) **PREEMPTION.**--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.

(d) **CONSULTATION.**--In carrying out this section, the Secretary of Health and Human Services shall consult with—

- (1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and
- (2) the Attorney General.

HIPAA Overview

Tentative Schedule for Publication of HIPAA Administrative Simplification Regulations

The Department of Health and Human Services (DHHS) is planning to issue HIPAA regulations under the following schedule. The time from publication of the Notice of Proposed Rule Making (NPRM) to publication of the final rule is needed to review and respond to the large number of comments received on the NPRMs. (For example, we received over 17,000 comments on the Transactions and Code Sets NPRM alone.) Both the logistics of handling the large volume of comments, and the analysis of the issues raised by the comments affect the time it takes to develop a final rule. Once written, the final rules must be reviewed by the Department of Health and Human Services and a number of its subordinate agencies, as well as by several other Federal departments affected by the rules. This schedule is, of course, subject to change. Where dates are missing, HHS has not yet set any specific target dates.

NPRMs Already Published:		
Standard	NPRM Published	Expected Final Rule Publication
Transactions and Code Sets	5/07/1998	Published August 17, 2000 Preamble Regulation Text
National Provider Identifier	5/07/1998	
National Employer Identifier	6/16/1998	
Security	8/12/1998	
Privacy	11/3/1999	Published December 28, 2000 Preamble (in 3 parts) Regulation Text

NPRMs in Development:			
Standard	Expected NPRM Publication	Expected Final Rule Publication	Expected Date Compliance Required*
National Health Plan Identifier			
Claims Attachments Enforcement			
National Individual Identifier	On hold.		
*Standards are required to be implemented generally within 2 years of the effective date of the final rule. (The effective date of the final rule is generally 60 days after its publication.) However, the effective date for the National Provider Identifier is likely to be delayed a few months to allow enough time for HHS to develop the system for implementing the identifier.			

Updated 12/28/2000

HIPAA Security: Protecting Patient Information

By: *Alan S. Goldberg* and *Steven J. Snyder*

On August 12, 1998 the Department of Health and Human Services published proposed regulations to implement certain of the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The goal is to develop and implement national standards and procedures for the electronic storage and transmission of health care information

The proposed regulations set forth a framework of standard minimum protocols and procedures for ensuring the safety, security and integrity of electronically stored and transmitted health care information. And, pursuant to Section 264 of HIPAA, if Congress does not enact legislation before August 21, 1999 to protect the privacy of protected health information, HCFA is required to promulgate regulations instead. Legislation is pending in both the House of Representatives and the Senate regarding the implementation of Section 262 (see, by way of example, the Medical Information Privacy and Security Act, H.R. 1057).

Whether or not the proposed regulations and pending legislation become law, the August 12, 1998 proposed regulations provide insight into and indicate the orientation of HCFA regarding how health information security should be managed. Eventually, the essence of these regulations likely will find its way into law, one way or another. Accordingly, physicians and those who provide services to physicians must understand the concerns and the inclinations of HCFA regarding health information and technology.

I. Who and What Would Be Regulated?

The focus of HIPAA and the proposed regulations is on the security of "Health Information", defined broadly to mean any information (whether oral or recorded in any medium) that relates to any of the following:

- (a) the past, present, or future physical or mental health or condition of an individual,
- (b) the provision of health care to an individual, or
- (c) the past, present, or future payment for the provision of health care to an individual.

The proposed regulations would affect any Health Information that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse. The breadth of these definitions encompasses nearly every record relating to health care (other than an individual's personal memorialization of health care delivered to herself or her family).

HIPAA Overview

New standards would apply to three categories of entities:

- (i) "Health Plans," meaning "any individual or group health plan that provides, or pays the costs of medical care" and including government sponsored health insurance and health care programs such as the Medicare and Medicaid programs, CHAMPUS, the Indian Health Service and the like, and Medicare supplement programs, all HMOs and similar state-regulated entities such as PPOs, medical foundations and competitive medical plans, all licensed insurance companies subject to state oversight and all employee welfare benefit programs and group health plans sponsored by employers.
- (ii) "Health Care Clearinghouses" (if engaged in certain electronic transmission activities) meaning entities that process healthcare information into standard data elements for electronic or other transmission, such as billing services, management information systems and community health information systems, and
- (iii) "Health Care Providers" (if engaged in certain electronic transmission activities) meaning any person or entity that furnishes or bills and is paid for health care services in the ordinary course of business. Note that only providers who maintain or transmit Health Information electronically (as opposed to on paper records and claims) would be subject to the proposed regulations.

Despite the caveats and limitations in the proposed regulations, just about every person or entity engaged in the electronic creation, transmission and storage of Health Information for other individuals would be subject to the HIPAA standards for data elements (when promulgated), security and electronic transmission.

II. Security Standards.

DHHS utilized extensive research into current marketplace security standards to develop the security standards in the proposed regulations. The security standards would not require the use of specific technologies or particular hardware or software, but instead would require Health Plans, Health Care Clearinghouses and Health Care Providers, who electronically store and transmit Health Information, to comply with certain minimum threshold protocols and procedures in four broad categories. These categories relate to different aspects of ensuring the integrity, confidentiality and availability of electronically stored and transmitted Health Information, as follows: (i) administrative procedures (ii) physical safeguards, (iii) technical protections relating to data storage and (iv) technical protections relating to access to and transmission of data.

The comments to the proposed regulations indicate that DHHS would require every element of compliance with each of the four categories to be documented, monitored, reviewed and regularly updated.

1. Administrative procedures to guard data integrity, confidentiality, and availability

HIPAA Overview

The proposed regulations would mandate in detail twelve distinct areas in which policies and procedures must be implemented and documented by every regulated entity, including (1) certification of data systems to evaluate compliance with security standards (DHHS apparently expects certification by third party entities), (2) "chain of trust" agreements among the regulated entity and each other entity with whom Health Information is exchanged, (3) a contingency plan to ensure continuity and preservation of data in the event of an emergency, (4) formal data processing protocols, (5) formal protocols for controlling access to data (6) internal audit procedures, (7) security features for initial clearance, ongoing supervision and training and overall monitoring of activity by personnel with access to Health Information, (8) "security configuration management" meaning procedures to coordinate overall security including documentation, hardware and software systems review, and virus checking, (9) protocols for reporting and responding to breaches of security, (10) establishment of a security management structure that features continuous risk assessment and thorough sanction policies and procedures, (11) specific procedures (such as changing locks and passwords) in the event of personnel terminations, and (12) training programs for all security management and process issues.

2. Physical safeguards to guard data integrity, confidentiality, and availability.

These requirements relate to the literal physical protection of data systems and data from intrusion and environmental hazards. Among other matters, regulated entities would be required to (1) formally assign security responsibility to a responsible person or entity, (2) develop controls on access to and the physical manipulation of hardware components such as disks, keyboards and monitors, (3) develop disaster and intrusion response and recovery plans, (4) implement personnel identification verification procedures for physical access to data sites, (5) maintain maintenance records (6) enforce security clearances hierarchies on a "need-to-know" basis, and (7) implement detailed protocols regarding activities and security at the work station level.

3. Technical security services to guard data integrity, confidentiality, and availability.

These requirements relate to software controls and protocols within and surrounding particular data systems to, among other things: (1) regulate access to particular privilege classes, including provision for emergency access during crises, (2) ensure internal systems audits and controls (3) provide for data authentication (to prove stored data is neither altered nor inappropriately accessed or processed) and (4) ensure user/communicator authentication and access control (using such methods as automatic log-off, user identification and other access controls such as biometric identification, passwords, a callback function or token-based systems).

4. Additional technical security mechanisms related to the transmission of data.

These requirements relate to software controls and protocols incident to electronic storage and transmission of Health Information to ensure that data cannot easily be accessed or intercepted or interpreted by unauthorized third parties. Proposed implementation features include (1) integrity controls (internal verification that data

HIPAA Overview

being transmitted or stored is valid) (2) message authentication (ensuring that the messages sent and received are the same), and (3) either access control to transmissions (such as dedicated lines secure from tampering) or encryption. If an entity chooses to attempt to control transmissions, rather than encryption, DHHS would also require (1) alarms to signal abnormal communication conditions, (2) automatic recording of audit trail information, and (3) a means of entity authentication.

The comments to the proposed regulations provide an extended narrative example illustrating how a small rural physician office might proceed in order to comply with the security standards. It is clear that significant time and resources will be necessary for even small providers to comply with the proposed new security standards.

III. Sanctions.

HIPAA mandates penalties for noncompliance with the standards at up to \$100 per person per violation up to \$25,000 per person for violations of a single standard for a calendar year. HIPAA also mandates criminal penalties for the knowing misuse of healthcare identifiers or obtaining or misusing of Health Information of up to \$50,000 and a year in prison with a higher penalty of \$100,000 and up to 5 years in prison if such offense is committed under false pretenses and up to \$250,000 or 10 years in prison if such offense is committed with "an intent to sell, transfer or use individually identifiable healthcare information for commercial advantage, personal gain or malicious harm".

The proposed regulations would mandate complex and resource-intensive efforts by nearly all health care providers, insurers and institutions, because even entities with sophisticated security protocols today would need to conduct audits and reviews to ensure compliance with the DHHS standards. The delivery of health care would be subject to sophisticated and demanding requirements in furtherance of heightened security, so that identifiable patient information would be protected and secure. Regardless whether these regulations are implemented in precisely the form summarized above, wise physicians will realize that the time for preparing for further computerization of medical information is now, and that the beginning of the end of primarily using DTM (that is, dead tree media) for the perpetuation of health information has begun. Only time will tell whether the proposed regulations will truly enhance privacy protections while preserving the ability of health care providers to access and use necessary patient information as and when necessary. Regardless of any enhancement, however, a new era in medical informatics is at hand, and things will never be the way they were again.

C:\HIPAA\Summary - Proposed Security regs.doc

HIPAA STANDARDS FOR ELECTRONIC HEALTH INFORMATION TRANSACTIONS:

SUMMARY OF HHS FINAL RULE

Background

Under the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), the Department of Health and Human Services (HHS) is required to adopt industry standards for the electronic transmission of health information. In May 1998, HHS issued a proposed rule to which there were about 17,000 comments, including comments from the American Hospital Association, American Medical Association, other physician groups, health plans, informatics firms, and others.

The final rule for implementation of the HIPAA standards for electronic transactions was put on display on August 11, 2000 and will be printed in the Federal Register August 17, 2000. The regulations become effective 60 days after publication. Covered entities (health plans, health care clearinghouses, and providers who transmit administrative data in electronic form) will have two years after that date to comply with the regulation (i.e., October 2002). Small health plans – those with a maximum of \$5 million in annual receipts—will have three years after that date to comply (i.e., October 2003). The new standards establish the content and formats to be used in submitting claims and other administrative data electronically between health care entities, including health care providers and health plans. HHS estimates the rule will provide a net savings to the health care industry totaling \$29.9 billion over 10 years (\$19.1 billion in savings when shown as discounted present value).

Section VII of the preamble for the final rule indicates that the rule has been released under the expectation that the privacy protections for personal health information will be in place by the rule's compliance date. If effective privacy standards are not in place, HHS will "seriously consider suspending the application of the transaction standards or taking action to withdraw this rule."¹

The rule and additional information on administrative simplification as well as on HIPAA more broadly is available on: <http://aspe.hhs.gov/admsimp/>

Changes from the Proposed Rule

Significant changes from the May 7, 1998 proposed rule include the following:

- The proposed rule included an exception from its application of standards for person-to-computer transactions (interactions between server to browser, direct data entry, fax back,

¹ The Clinton Administration is still intending to publish the final privacy rule later this year.

HIPAA Overview

etc.). This exception has been eliminated. These transmissions must use the adopted standard data elements and data content.

- The proposed rule distinguished between internal and external transactions, such as within and outside of corporate boundaries. The final rule eliminates this type of distinction and lays out a test for when the rule's standards must be used for transactions.
- The definition of a small health plan has been modified to mean one with a maximum of \$5 million in annual receipts. (The proposed rule had defined it as one with fewer than 50 participants.)
- There are many new definitions to clarify the applicability and scope of the rule.
- Language from the proposed rule was revised to state that a health plan may not delay the transaction or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the basis that the transaction is a standard transaction (and thus subject to these rules). A forthcoming enforcement rule will address the penalties for violating the HIPAA requirements. Separate privacy and security regulations are being prepared that will address these issues as they relate to health information.
- Exceptions from HIPAA's federal preemption of state law will be addressed in the forthcoming final rule for privacy standards.
- Various assumptions and data were modified in the impact analysis contained in the final rule. Most importantly, HHS has projected costs and benefits of implementation for covered entities on the basis of 10 years instead of 5 years. As explained in the preamble, the major costs for plans and purchasers of purchasing new systems and conforming to the standards are in the near-term whereas savings in reduced transaction costs will increase over the long-term. Thus, the 10-year window provides for a higher estimate of system-wide savings. The gross cost of implementation has increased from \$5.8 billion to \$7 billion; the gross savings have increased from \$29.9 billion to \$36.9 billion. The net savings have increased from \$24.2 billion to \$29.9 billion. (See Impact Tables at end of document.)

Summary of the Final Rule

According to HHS, there are currently about 400 formats for electronic health care claims processing in use nationwide. The lack of standardization makes it difficult and expensive to develop and maintain software and reduces the ability of health care providers and plans to achieve efficiency and savings in administrative transactions. The intent of HIPAA's administrative simplification provision is to streamline administrative transactions by moving to national standards developed by private industry for the transmission of electronic health data. By providing for national standards for electronic claims and other administrative transactions, health care providers will be able to submit the same transaction to any health plan in the country and the health plan will have to accept it. Health plans will be able to send standard electronic transactions such as remittance advices and referral authorizations to health care providers. The

HIPAA Overview

result will be substantial savings in administrative costs for plans and providers, especially over the long term.

Application of Rule. The regulation applies to every health plan and to every health care clearinghouse. It also applies to every health care provider who transmits any administrative health information (as listed below) in electronic form.

As defined under the statute, “health plan” is used very broadly to include all public (e.g., Medicare, Medicaid, FEHBP, VA, military health care, and Indian Health Care), and most private health plans. The major exception is self-administered, employer-sponsored group health plans under 50 employees.

A health care “clearinghouse” is a public or private entity that does either of the following: (1) processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or (2) receives a standard transaction from another entity and processes or facilitates the processing of information into nonstandard format or nonstandard data content for a receiving entity.

Transactions within the boundaries of a corporate entity are subject to the requirements of the rule, just as they are between such entities. This is a change from the earlier proposal to exempt transmissions within a corporate entity to reduce burden. “We have not been able to define ‘corporate entity’ so that the exception would not defeat the rule,” HHS states in the preamble to the rule. HHS further asserts that this decision does not impose an additional burden on health plans, “because health plans already are required to have the capacity to accept standard transactions from any person.”

As required under HIPAA, transactions that are required to use the standards under this regulation are:

1. Health claims and equivalent encounter information
2. Enrollment and disenrollment in a health plan
3. Eligibility for a health plan
4. Health care payment and remittance advice
5. Health plan premium payments
6. Health claim status
7. Referral certification and authorization
8. Coordination of benefits.

Federal Preemption of State laws. HIPAA provides that standards for transactions will supersede any state law that is contrary to them. However, it also allows an exceptions process if the Secretary determines that the provision of state law is necessary to prevent fraud and abuse,

HIPAA Overview

ensure appropriate state regulation of insurance and health plans, among other things. This process is currently under development and will be issued in the final rule for privacy standards.²

Modifications. With exceptions, HIPAA requires the Secretary to review the adopted standards and adopt modifications (including additions) as determined appropriate, but no more frequently than once every 12 months. In the first year after a standard is adopted, however, the Secretary may adopt a modification if she determines that such modification is necessary to permit compliance with the standard.

Effective Dates. Covered entities must comply with the applicable requirements no later than 24 months after the effective date of the final rule in the *Federal Register*. (The effective date is 60 days after its publication. Therefore, compliance with the final rule is required by October 2002. Small health plans have until 36 months after the effective date of the final rule (October 2003). Entities can begin using the standards earlier than the compliance date.

General Requirement. If a covered entity conducts with another covered entity (or within the same covered entity), using electronic media, a transaction for which the Secretary has adopted a standard, the covered entity must conduct the transaction as a standard transaction.

A “standard” means a prescribed set of rules, conditions or requirements describing the following information for products, systems, services, or practices: (1) classification of components, (2) specification of materials, performance, or operations, and (3) delineation of procedures. An exception to this requirement applies in the case of direct data entry transactions. A health care provider electing to use direct data entry offered by a health plan to conduct an administrative transaction for which a standard has been adopted must use the applicable *data content* and *data condition* requirements of the standard when conducting the transition. The provider is not, however, required to use the *format* requirements of the standard. (This situation arises, for example, when a physician directly submits a claim to a health plan using the plan’s data entry system installed in the doctor’s office.) If a covered entity uses a business associate, such as health care clearinghouse, to conduct an electronic transaction covered under this rule, then the covered entity must require the business associate (or any of its subcontractors) to comply with the applicable requirements of this rule.

Additional Requirements for Health Plans. If an entity requests a health plan to conduct a transaction as a standard transaction, then the health plan must do so, and cannot in any way delay or reject such a transaction.³ It cannot reject the transaction because it contains excess or unneeded data elements. It may not offer an incentive for a health care provider to conduct a transaction as a direct data entry (and therefore not subject to all of the requirements). A health plan that operates as a health care clearinghouse or requires an entity to use one may not charge

² See: *FAQs about Standards for Electronic Transaction*, <http://aspe.hhs.gov/admsimp/faqtx.htm>

³ As stated in the preamble of the regulation, “a health plan is required to have the capacity to accept and/or send (either by itself, or by hiring a health care clearinghouse to accept and/or send on its behalf) a standard transaction that it otherwise conducts but does not currently support electronically. . . .”

HIPAA Overview

fees or costs in excess of fees or costs for normal telecommunications that the entity incurs when it directly transmits or receives a standard transaction.

Additional rules are also specified for health care clearinghouses.

Code Sets. When conducting a transaction covered by this rule, a covered entity must use the applicable medical code and nonmedical code data sets that are specified under the rule. A “code set” is any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes, or medical procedure codes.

The code sets adopted by the Secretary under this regulation include:

- (1) ICD-9-CM, volumes I and II, for diseases, injuries, impairments, etc;
- (2) ICD-9-CM, volume 3, Procedures, for procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals;
- (3) National Drug Codes for drugs and biologics;
- (4) Code on Dental Procedures and Nomenclature for dental services;
- (5) Combination of Health Care Financing Administration Common Procedure Coding System (HCPCS) and Current Procedural Terminology (CPT-4) for physician services and other health care services (e.g., physical and occupational services, radiologic procedures, etc.; and
- (6) Health Care Financing Administration Common Procedure Coding System (HCPCS) for all other substances, equipment, supplies or other items used in health care services.

Health Care Claims or Equivalent Encounter Information. Transactions of claims or equivalent information means the transmission of either of the following: (1) a request to obtain payment, and the necessary accompanying information from a health care provider to a health plan, for health care; and (2) if there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care. The following industry-developed standards for claims or equivalent information have been adopted:

1. Institutional health care claims: *The ASC X12N 837 – Health Care Claim: Institutional*, Volumes 1 and 2, Version 4010, May 2000. (ASC is the Accredited Standards Committee.)
2. Professional health care claims: *The ASC X12N 837 - – Health Care Claim: Professional*, Volumes 1 and 2, Version 4010, May 2000.
3. Dental health care claims: *The ASC X12N 837 - – Health Care Claim: Dental*, Version 4010, May 2000.
4. Retain pharmacy drug claims. *The National Council for Prescription Drug Programs (NCPDP) Telecommunications Standard Implementation Guide*, Version 5, Release 1, September 1999 and *equivalent NCPDP Standard Batch Implementation Guide*, Version 1, Release 0, February 1, 1996.

HIPAA Overview

Standards are also specified in the same manner for electronic transactions related to health plan eligibility; referral certification and authorization; health care claim status; enrollment and disenrollment in a health plan; payment and remittance; health plan premium payments; and coordination of benefits.

All of these standards have been developed by private sector standards development organizations accredited by the American National Standards Institute (ANSI). Information on obtaining the standards listed above is provided in §162.920(1)(1) of the regulation.

Effects on Physicians. Some physicians have expressed concern that they would have to buy computers to comply with the administrative simplification requirements. As stated in the HHS guidance accompanying the rule, there is no such requirement. However, “physicians may **want** to use computers for submitting and receiving transactions (such as health care claims and remittances/payments) electronically, once the standard way of doing things goes into effect.”⁴ More broadly, neither HIPAA nor the final rule for electronic transactions requires physicians to submit transactions electronically. But if they are submitted electronically, such transmissions must comply with the standards specified in this regulation.

Another issue that arose with respect to the proposed rule whether a physician or other health care provider electing to transmit some data electronically would then have to transmit all covered administrative data electronically. The preamble to the final rule adopts the same language as in the statute “a health care provider who transmits any health information in electronic form in connection with a transaction” referred to in the HIPAA requirement. It goes on to provide the following example: A provider may send an electronic health care claim or equivalent encounter information standard for Patient A to health plan Z, and may send a paper claim for Patient B to health plan Z. A provider may also send an electronic claim or equivalent encounter information standard transaction to health plan S and then send paper claims to health plan T.

C:\HIPAA\Summary - Transaction standards.doc

⁴ FAQs about Standards for Electronic Transactions, <http://aspe.hhs.gov/admsimp/faqt.htm>

Privacy Regulations HHS Fact Sheet

May 9, 2001

Contact: HHS Press Office
(202) 690-6343

PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION

Overview: *Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality.*

Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that information. The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact such legislation after three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes in order to address issues raised by the comments. To ensure that the provisions of the final rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to care or quality of care, HHS Secretary Tommy G. Thompson opened the final rule for comment for 30 days. After that comment period, President Bush and Secretary Thompson decided to allow the rule to take effect on April 14, 2001, as scheduled, and make appropriate changes in the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care. Secretary Thompson's statement on this issue is available at <http://www.hhs.gov/news/press/2001pres/20010412.html>.

COMPLIANCE SCHEDULE

The final rule took effect on April 14, 2001. As required by the HIPAA law, most covered entities have two full years - until April 14, 2003 - to comply with the final rule's provisions. The law gives HHS the authority to make appropriate changes to the rule prior to the compliance date.

HIPAA Overview

COVERED ENTITIES

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

INFORMATION PROTECTED

All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

CONSUMER CONTROL OVER HEALTH INFORMATION

Under the final rule, patients will have significant new rights to understand and control how their health information is used.

- **Patient education on privacy protections.** Providers and health plans will be required to give patients a clear written explanation of how the covered entity may use and disclose their health information.
- **Ensuring patient access to their medical records.** Patients will be able to see and get copies of their records, and request amendments. In addition, a history of non-routine disclosures must be made accessible to patients.
- **Receiving patient consent before information is released.** Health care providers who see patients will be required to obtain patient consent before sharing their information for treatment, payment, and health care operations. In addition, separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients will have the right to request restrictions on the uses and disclosures of their information.
- **Providing recourse if privacy protections are violated.** People will have the right to file a formal complaint with a covered provider or health plan, or with HHS, about violations of the provisions of this rule or the policies and procedures of the covered entity.

BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

With few exceptions, such as appropriate law enforcement needs, an individual's health information may only be used for health purposes.

- **Ensuring that health information is not used for non-health purposes.** Health information covered by the rule generally may not be used for purposes not related to health care - such as disclosures to employers to make personnel decisions, or to financial institutions - without explicit authorization from the individual.
- **Providing the minimum amount of information necessary.** In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes because physicians, specialists, and other providers need access to the full record to provide quality care.

HIPAA Overview

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives covered entities the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources. Covered entities generally will have to:

- **Adopt written privacy procedures.** These include who has access to protected information, how it will be used within the entity, and when the information may be disclosed. Covered entities will also need to take steps to ensure that their business associates protect the privacy of health information.
- **Train employees and designate a privacy officer.** Covered entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORDS USE AND RELEASE

In HIPAA, Congress provided penalties for covered entities that misuse personal health information.

- **Civil penalties.** Health plans, providers and clearinghouses that violate these standards will be subject to civil liability. Civil money penalties are \$100 per violation, up to \$25,000 per person, per year for each requirement or prohibition violated.
- **Federal criminal penalties.** Under HIPAA, Congress also established criminal penalties for knowingly violating patient privacy. Criminal penalties are up to \$50,000 and one year in prison for obtaining or disclosing protected health information; up to \$100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

BALANCING PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

In limited circumstances, the final rule permits - but does not require - covered entities to continue certain existing disclosures of health information without individual authorization for specific public responsibilities.

These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security.

All of these disclosures could occur today under existing laws and regulations, although the privacy rule generally establishes new safeguards and limits. If there is no other law requiring that information be disclosed, covered entities will use their professional judgments to decide whether to disclose any information, reflecting their own policies and ethical principles.

HIPAA Overview

SPECIAL PROTECTION FOR PSYCHOTHERAPY NOTES

Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection because they are not part of the medical record and are never intended to be shared with anyone else. All other personal health information is considered to be sensitive and protected consistently under this rule.

EQUIVALENT REQUIREMENTS FOR GOVERNMENT ENTITIES

The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government medical units have to comply with the full range of requirements, such as providing notice, access rights and requiring consent for routine uses.

COST OF IMPLEMENTATION

The final rule projected the implementation costs at \$17.6 billion over 10 years - a figure more than offset by the \$29.9 billion in projected savings under the final electronic transactions regulation issued in August 2000.

PRESERVING EXISTING, STRONG STATE CONFIDENTIALITY LAWS

As required by the HIPAA law itself, stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule will set a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information, the final rule does not preempt these mandates.

COMPLIANCE AND ENFORCEMENT

The final rule will be enforced by the HHS Office for Civil Rights (OCR). Before covered entities must comply with the rule, OCR will provide assistance to providers, plans and health clearinghouses in meeting the requirements of the regulation. A Web site on the new regulation is available at <http://www.hhs.gov/ocr/hipaa/>.

###

Note: All HHS press releases, fact sheets and other press materials are available at <http://www.hhs.gov/news>.

HIPAA Overview

Final HIPAA Privacy Regulations Analytical Outline

Basic Rule of Nondisclosure - A covered entity may not use or disclose an individual's protected health information, except as otherwise permitted or required by this subpart." § 164.502(a).	82805
What and Who are covered?	
160.102 Applicability	82798
160.103 Definitions	82798
164.500 Applicability	82802
164.501 Definitions	82803
The Basic Rule	
164.502 Uses & Disclosures of Protected Health Information: General Rules	82805
a) Standard: permitted & required disclosures	82805
Exception to Nondisclosure #1 – Consent	
164.506 Consent for uses or disclosures to carry out treatment, payment or health care operations	82810
a) Standard: consent requirement	82810
b) Implementation specifications: general requirements	82810
c) Implementation specifications: content requirements	82810
d) Implementation specifications: defective consents	82810
e) Standard: resolving conflicting consents and authorizations	82810
f) Standard: joint consents	82811
Exception to Non-disclosure #2 – Authorization	
164.508 Uses and disclosures for which an authorization is required	82811
a) Standard: authorization for uses and disclosures	82811
b) Implementation specifications: general requirements	82811

HIPAA Overview

	c) Implementation specifications: core element and plain language requirement	82811
	d) Implementation specifications: authorizations requested by a covered entity for its own uses and disclosures	82812
	e) Implementation specifications: authorizations requested by a covered entity for disclosures by others	82812
	f) Implementation specifications: authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual	82812
Exception to Non-disclosure #3 – “Opt-Out”		
	164.510 Uses and disclosures requiring an opportunity for the individual to agree/object	82812
	a) Standard: use and disclosure for facility directories	82812
	b) Standard: uses and disclosures for involvement in the individual's care and notification purposes	.
Exception to Non-disclosure #4 – Exceptions		
	164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree/object is not required	82813
	a) Standard: required by law	82813
	b) Standard: public health activities	82813
	c) Standard: victims of abuse, neglect or domestic violence	82814
	d) Standard: health oversight activities	82814
	e) Standard: judicial and administrative proceedings	82814
	f) Standard: law enforcement purposes	82815
	g) Standard: decedents	82816
	h) Standard: organ, eye, tissue donation	82816
	i) Standard: research purposes	82816
	j) Standard: to avert serious threat to health or safety	82817
	k) Standard: specialized government functions	82817
	l) Standard: worker's compensation	82818

HIPAA Overview

Exception to Non-disclosure #5 – Patients		
	164.524 Access of individuals to protected health information	82823
	a) Standard: access to protected health information	82823
	b) Implementation specifications: requests for access and timely action	82823
	c) Implementation specifications: provision of access	82824
	d) Implementation specifications: denial of access	82824
	e) Implementation specifications: documentation	82824
Additional Patient Rights		
	164.520 Notice of privacy protections of protected health information	82820
	a) Standard: notice of privacy practices	82820
	b) Implementation specifications: content of notice	82821
	c) Implementation specifications: provision of notice	82821
	d) Implementation specifications: joint notice by separate covered entities	82822
	e) Implementation specifications: documentation	82822
	164.522 Rights to request privacy protection for protected health information	82822
	a) Standard: right of an individual to request restriction of uses and disclosures	82822
	b) Standard: confidential communications requirements	82823
	164.526 Amendment of protected health information	82824
	a) Standard: right to amend	82824
	b) Implementation specifications: requests for amendment and timely action	82825
	c) Implementation specifications: accepting the amendment	82825
	d) Implementation specifications: denying the amendment	82825
	e) Implementation specifications: actions on notices of amendment	82825
	f) Implementation specifications: documentation	82825

HIPAA Overview

	164.528 Accounting of disclosures of protected health information	82826
	a) Standard: right to an accounting of disclosures of protected health information	82826
	b) Implementation specifications: content of the accounting	82826
	c) Implementation specifications: provision of the accounting	82826
	d) Implementation specifications: documentation	82826
Administrative Requirements		
	164.530 Administrative requirements	82826
	a) Standard: personnel designation	82826
	b) Standard: training	82826
	c) Standard: safeguards	82827
	d) Standard: complaints to the covered entity	82827
	e) Standard: sanctions	82827
	f) Standard: mitigation	82827
	g) Standard: refraining from intimidating or retaliatory acts	82827
	h) Standard: waiver of rights	82827
	i) Standard: policies and procedures	82827
	j) Standard: documentation	82828
	k) Standard: group health plans	82828
	164.502 Uses & Disclosures of Protected Health Information: General Rules	82805
	b) Standard: minimum necessary	82805
	c) Standard: uses & disclosures of protected health information subject to an agreed upon restriction	82806
	d) Standard: uses & disclosures de-identified protected health information	82806
	e) Standard: disclosures to business associates	82806
	f) Standard: deceased	82806
	g) Standard: personal representatives	
	h) Standard: confidential communications	82806
	i) Standard: uses & disclosures consistent with notice	
	j) Standard: disclosures by whistle blowers and work force member crime victims	82807

HIPAA Overview

	164.504 Uses & Disclosures: organizational requirements	82807
	a) Definitions	82807
	b) Standard: healthcare component	82807
	c) Implementation Specification: hybrid entity	
	d) Standard: affiliated covered entities	82808
	e) Standard: business associate contracts	82808
	f) Standard: requirements for group health plans	82809
	g) Standard: requirements for a covered entity with multiple covered functions	82809
	164.514 Other requirements related to uses and disclosures of protected health information	82818
	a) Standard: de-identification of protected health information	82818
	b) Implementation specifications: requirements for de-identification of protected health information	82818
	c) Implementation specifications: re-identification	82819
	d) Standard: minimum necessary requirements	82819
	e) Standard: marketing	82819
	f) Standard: fundraising	82820
	g) Standard: underwriting and related purposes	82820
	h) Standard: verification requirements	82820
Technical Provisions		
	Preemption of State Law	82800
	160.201 Applicability	82800
	160.202 Definitions	82800
	160.203 General Rule and Exceptions	82801
	160.204 Process for requesting exception determinations	82801
	160.205 Duration of effectiveness of exception determinations	82801
	Compliance and Enforcement	82801
	160.300 Applicability	82801
	160.302 Definitions	82801

HIPAA Overview

	160.304 Principles for achieving compliance	82801
	160.306 Complaints to the Secretary	82801
	160.308 Compliance reviews	82802
	160.310 Responsibilities of covered entities	82802
	160.312 Secretarial action regarding complaints and compliance reviews	82802