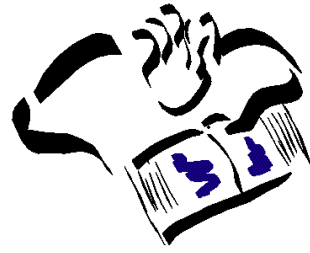


Phaedrus Company and mdconsult.net have compiled this resource as an overview to the coming HIPAA privacy standards to help health industry professionals make sense of coming changes.



Phaedrus Company and mdconsult.net have compiled the information in this document from sources believed to be reliable regarding patient information privacy standards and expectations for implementation of HIPAA.

However, Phaedrus Company and mdconsult.net make no warranties whatsoever regarding this document, and hereby disclaim all warranties whatsoever, either express or implied, that the information contained in this document is complete or accurate or that adherence to guidelines will absolve legal liability. Phaedrus Company and mdconsult.net make no warranty as to the reliability, accuracy, timeliness, usefulness, adequacy, completeness or suitability of the information and suggestions in this document.

UNDER NO CIRCUMSTANCES SHALL Phaedrus Company and mdconsult.net OR ANY OTHER PARTY INVOLVED IN CREATING, PRODUCING OR DISTRIBUTING THIS DOCUMENT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES WHATSOEVER, INCLUDING BUT NOT LIMITED TO THOSE FOR LOSS OF PROFITS, GOODWILL OR OTHER INTANGIBLE LOSSES THAT RESULT FROM THE USE OF INFORMATION CONTAINED IN THIS DOCUMENT.

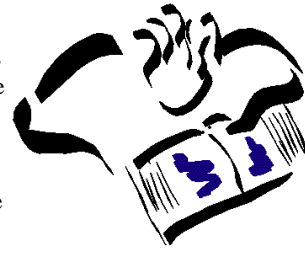
phaedrus
C O M P A N Y

mdconsult.net

15 Corporate Ridge • Suite 15 • Hamden, CT 06514 • (203) 314-7763
www.phaedrusco.com • www.mdconsult.net

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.

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.

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. Self-administered employee health benefit plans and plans with fewer than 50 participants are excluded.

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.

phaedrus
C O M P A N Y

mdconsult.net

15 Corporate Ridge • Suite 15 • Hamden, CT 06514 • (203) 314-7763
www.phaedrusco.com • www.mdconsult.net

Boundaries on Medical Records 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.

Ensure the Security of Personal 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.

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.

phaedrus
C O M P A N Y

mdconsult.net

15 Corporate Ridge • Suite 15 • Hamden, CT 06514 • (203) 314-7763
www.phaedrusco.com • www.mdconsult.net

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 State 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 - including a toll free line to help answer questions: 1-866-OCR-PRIV (1-866-627-7748). The TTY number is 1-866-788-4989.

phaedrus
C O M P A N Y

mdconsult.net

15 Corporate Ridge • Suite 15 • Hamden, CT 06514 • (203) 314-7763
www.phaedrusco.com • www.mdconsult.net