

# HHS Fact Sheet

U.S. Department of Health and Human Services



[www.hhs.gov/news](http://www.hhs.gov/news)

December 20, 2000

Contact: HHS Press Office  
(202) 690-6343

## PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION SUMMARY OF THE FINAL REGULATION

---

**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. For many years, the confidentiality of those records was maintained by our family doctors, who kept our records sealed away in file cabinets and refused to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving large gaps in the protection of patients' privacy and confidentiality. There is a pressing need for national standards to control the flow of sensitive patient information and to establish real penalties for the misuse or disclosure of this information.*

*President Clinton and 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). That law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. After three years of discussion in Congress without passage of such a law, HIPAA provided HHS with the authority to craft such privacy protections by regulation. Following the principles and policies laid out in the recommendations for national health information privacy legislation the Administration submitted to Congress in 1997, the Administration drafted regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records and the President and Secretary Donna E. Shalala released them in October of last year. During an extended comment period, HHS received, electronically or on paper, more than 52,000 communications from the public.*

*This final rule provides the first comprehensive federal protection for the privacy of health information. However, because of the limitations of the HIPAA statute, these protections do not fully achieve the Administration's goal of a seamless system of privacy protection for all health information. Members of both parties in Congress will need to pass meaningful, comprehensive privacy protection for American patients that would extend the reach of the standards being finalized today to all entities that hold personal health information.*

## **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 held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally, is covered by the final regulation.

## **COMPONENTS OF THE FINAL RULE**

The rule is the result of the Department's careful consideration of every comment and reflects a balance between accommodating practical uses of individually identifiable health information and rendering maximum privacy protection of that information.

## **CONSUMER CONTROL OVER HEALTH INFORMATION**

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

- Patient education on privacy protections. Providers and health plans are required to give patients a clear written explanation of how they can use, keep, and disclose their health information.
- Ensuring patient access to their medical records. Patients must be able to see and get copies of their records, and request amendments. In addition, a history of most disclosures must be made accessible to patients.
- Receiving patient consent before information is released. Patient authorization to disclose information must meet specific requirements. Health care providers who see patients are required to obtain patient consent before sharing their information for treatment, payment, and health care operations purposes. In addition, specific patient consent must be sought and granted for non-routine uses and most non-health care purposes, such as releasing information to financial institutions determining mortgages and other loans or selling mailing lists to interested parties such as life insurers. Patients have the right to request restrictions on the uses and disclosures of their information.
- Ensuring that consent is not coerced. Providers and health plans generally cannot condition treatment on a patient's agreement to disclose health information for non-routine uses.
- Providing recourse if privacy protections are violated. People have the right to complain to a covered provider or health plan, or to the Secretary, 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, an individual's health information can be used for health purposes only.

- Ensuring that health information is not used for non-health purposes. Patient information can be used or disclosed by a health plan, provider or clearinghouse only for purposes of health care treatment, payment and operations. Health information cannot be used for purposes not related to health care - such as use by employers to make personnel decisions, or use by financial institutions - without explicit authorization from the individual.
- Providing the minimum amount of information necessary. Disclosures of information must be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the transfer of medical records for purposes of treatment, since physicians, specialists, and other providers need access to the full record to provide best quality care.
- Ensuring informed and voluntary consent. Non-routine disclosures with patient authorization must meet standards that ensure the authorization is truly informed and voluntary.

### **ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION**

The regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, implementation of the standards will be flexible and scalable, to account for the nature of each entity's business, and its size and resources. Covered entities must:

- Adopt written privacy procedures. These must include who has access to protected information, how it will be used within the entity, and when the information would or would not be disclosed to others. They must also take steps to ensure that their business associates protect the privacy of health information.
- Train employees and designate a privacy officer. Covered entities must provide sufficient training so that their employees understand the new privacy protection procedures, and designate an individual to be responsible for ensuring the procedures are followed.
- Establish grievance processes. Covered entities must provide a means for patients to make inquiries or complaints regarding the privacy of their records.

### **ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORDS USE AND RELEASE**

Penalties for covered entities that misuse personal health information are provided in HIPAA.

- Civil penalties. Health plans, providers and clearinghouses that violate these standards would be subject to civil liability. Civil money penalties are \$100 per incident, up to \$25,000 per person, per year, per standard.
- Federal criminal penalties. There would be federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. 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**

After balancing privacy and other social values, HHS is establishing rules that would permit certain existing disclosures of health information without individual authorization for the following national priority activities and for activities that allow the health care system to operate more smoothly. All of these disclosures have been permitted under existing laws and regulations. Within certain guidelines found in the regulation, covered entities may disclose information for:

- Oversight of the health care system, including quality assurance activities
- Public health
- Research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board
- Judicial and administrative proceedings
- Limited law enforcement activities
- Emergency circumstances
- For identification of the body of a deceased person, or the cause of death
- For facility patient directories
- For activities related to national defense and security

The rule permits, but does not require these types of disclosures. If there is no other law requiring that information be disclosed, physicians and hospitals will still have to make judgments about whether to disclose information, in light of 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 never intended to be shared with anyone else. All other health information is considered to be sensitive and treated consistently under this rule.

**EQUIVALENT TREATMENT OF PUBLIC AND PRIVATE SECTOR HEALTH PLANS AND PROVIDERS.** The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government agency medical units must comply with the full range of requirements, such as providing notice, access rights, requiring consent before disclosure for routine uses, establishing contracts with business associates, among others.

### **CHANGES FROM THE PROPOSED REGULATION**

- Providing coverage to personal medical records in all forms. The proposed regulation had applied only to electronic records and to any paper records that had at some point existed in electronic form. The final regulation extends protection to all types of personal health information created or held by covered entities, including oral communications and paper records that have not existed in electronic form. This creates a privacy system that covers virtually all health information held by hospitals, providers, health plans and health insurers.
- Requiring consent for routine disclosures. The final rule requires most providers to obtain patient consent for routine disclosure of health records, in addition to requiring special patient authorization for non-routine disclosures. The earlier version had proposed allowing these routine disclosures without advance consent for purposes of treatment, payment and health care operations (such as internal data gathering by a provider or health care plan). However, most individuals commenting on this provision, including many physicians, believed consent for these purposes should be obtained in advance, as is typically done today. The final rule retains the new requirement that patients must also be provided detailed written information on privacy rights and how their information will be used.
- Allowing disclosure of the full medical record to providers for purposes of treatment. For most disclosures, such as information submitted with bills, covered entities are required to send only the minimum information needed for the purpose of the disclosure. However, for purposes of treatment, providers need to be able to transmit fuller information. The final rule gives providers full discretion in determining what personal health information to include when sending patients' medical records to other providers for treatment purposes.
- Protecting against unauthorized use of medical records for employment purposes. Companies that sponsor health plans will not be able to access the personal health information held by the plan for employment-related purposes, without authorization from the patient.

### **COST OF IMPLEMENTATION**

Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress provided in HIPAA 1996 that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year \$29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected \$17.6 billion in costs projected for the privacy regulation. This produces a net savings of approximately \$12.3 billion for the health care delivery system while improving the efficiency of health care as well as privacy protection.

### **PRESERVING EXISTING, STRONG STATE CONFIDENTIALITY LAWS**

Stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule sets 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 for civic purposes, we do

not preempt these mandates. The result is to give individuals the benefit of all laws providing confidentiality protection as well as to honor state priorities.

### **THE NEED FOR FURTHER CONGRESSIONAL ACTION**

HIPAA limits the application of our rule to the covered entities. It does not provide authority for the rule to reach many persons and businesses that work for covered entities or otherwise receive health information from them. So the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information. There is no statutory authority for a private right of action for individuals to enforce their privacy rights. We need Congressional action to fill these gaps in patient privacy protections.

### **IMPLEMENTATION OF THE FINAL REGULATION**

The final regulation will come into full effect in two years. The regulation will be enforced by HHS' Office for Civil Rights, which 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. A Web site on the new regulation will also be available at <http://www.hhs.gov/ocr>.

###

---

Note: For other HHS Press Releases and Fact Sheets pertaining to the subject of this announcement, please [click here](#) for our Press Release and Fact Sheet search engine at: <http://www.hhs.gov/search/press.html>.

## HIPAA FINAL PRIVACY RULE

CFR(code of Federal regulations)-CITATION	REQUIREMENTS
164.518(a)	<p><b>Designation of Privacy Official and Contact Person</b>  <sup>1</sup>(Responsible for: development; implementation of entity's privacy policies and procedures)</p> <ul style="list-style-type: none"> <li>a. Designation of a Contact Person to receive complaints about privacy and matters covered by entity's notice</li> <li>b. Privacy Official and Contact Person can be but are not required to be the same individual</li> </ul>
164.518(b)	<p><b>Training</b>            Provide training on the entity's policies and procedures to all employees having access to protected health information</p> <ul style="list-style-type: none"> <li>a. Initial training by compliance date of rule</li> <li>b. New employee training within reasonable time</li> <li>c. Documentation that training has been provided</li> </ul>
164.518(c)	<p><b>Safeguards</b>            Covered Entities are required to safeguard protected health information from accidental or intentional use or disclosure and to protect against inadvertent disclosure to persons other than the intended recipient<sup>2</sup></p> <ul style="list-style-type: none"> <li>a. Extends coverage to both paper and electronic records</li> <li>b. Safeguards must be appropriate and require<sup>3</sup> <ul style="list-style-type: none"> <li>1. Shredding of paper documents before disposal</li> <li>2. Locks on file cabinets</li> <li>3. Uses of keys or pass codes for personnel</li> </ul> </li> <li>c. Verify the identity and authority of persons(other than employees) to whom they make disclosures.</li> </ul>
164.518(d)	<p><b>Complaints to Covered Entity</b>            Must have mechanism for receiving complaints</p> <ul style="list-style-type: none"> <li>a. Identify contact person</li> <li>b. Document complaints received and dispositions</li> </ul>
164.520	<p><b>Policies and Procedures and Documentation</b>            Covered entities must maintain in writing all policies and procedures , communications, actions or activities pertaining to the establishment of and implementation of health information privacy provision</p> <ul style="list-style-type: none"> <li>a. Documentation must be retained for 6 years</li> <li>b. Writing only specifies electronic records</li> </ul>
164.514(a)-(c)	<p><b>Uses and Disclosures-De-Identification</b></p> <ul style="list-style-type: none"> <li>a. All electronic records that identify individuals be fixed               <ul style="list-style-type: none"> <li>1. Stripped of direct identifiers: name; address; phone numbers; Social Security number; Driver's license number; Motor vehicle registration; Voter registration number; Finger prints; Voice prints; Web universal resource locator; and, IP address number</li> <li>2. Meet the "reasonable basis" statutory standard</li> <li>3. Or can use method described in Statistical Policy Working Paper<sup>22</sup>-Report on Statistical Disclosure<sup>4</sup> Limitation Methodology</li> </ul> </li> </ul>

<sup>1</sup> Requirements consistent with approach recommended by JCAHO and NCQA in paper," Protecting Personal Health Information; A framework for Meeting the Challenges in a Managed Care Environment"

<sup>2</sup> Covered entities are(1) **health plans**, (2) **health care clearinghouses**, and (3) **health care providers** who transmit health information in electronic form in connection with transactions

<sup>3</sup> ASTM and AHIMA have developed a body of recommended practices for handling protected health information cited in Final Rule

<sup>4</sup> Federal Committee on Statistical Methodology, Office of Management and Budget