



PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION

OVERVIEW: The first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003. Developed by the Department of Health and Human Services (HHS), these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule.

Congress called on HHS to issue patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA included provisions designed to encourage electronic transactions and also required new safeguards to protect the security and confidentiality of health information. The final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., enrollment, billing and eligibility verification) electronically. Most health insurers, pharmacies, doctors and other health care providers were required to comply with these federal standards beginning April 14, 2003. As provided by Congress, certain small health plans have an additional year to comply. HHS has conducted extensive outreach and provided guidance and technical assistance to these providers and businesses to make it as easy as possible for them to implement the new privacy protections. These efforts include answers to hundreds of common questions about the rule, as well as explanations and descriptions about key elements of the rule. These materials are available at <http://www.hhs.gov/ocr/hipaa>.

PATIENT PROTECTIONS

The new privacy regulations ensure a national floor of privacy protections for patients by limiting the ways that health plans, pharmacies, hospitals and other covered entities can use patients' personal medical information. The regulations protect medical records and other individually identifiable health information, whether it is on paper, in computers or communicated orally. Key provisions of these new standards include:

- **Access To Medical Records.** Patients generally should be able to see and obtain copies of their medical records and request corrections if they identify errors and mistakes. Health plans, doctors, hospitals, clinics, nursing homes and other covered entities generally should provide access these records within 30 days and may charge patients for the cost of copying and sending the records.
- **Notice of Privacy Practices.** Covered health plans, doctors and other health care providers must provide a notice to their patients how they may use personal medical information and their rights under the new privacy regulation. Doctors, hospitals and other direct-care providers generally will provide the notice on the patient's first visit following the April 14, 2003, compliance date and upon request. Patients generally will be asked to sign, initial or otherwise acknowledge that they received this notice. Health plans generally must mail the notice to their enrollees by April 14 and again if the notice changes significantly. Patients also may ask covered entities to restrict the use or disclosure of their information beyond the practices included in the notice, but the covered entities would not have to agree to the changes.
- **Limits on Use of Personal Medical Information.** The privacy rule sets limits on how health plans and covered providers may use individually identifiable health information. To promote the best quality care for patients, the rule does not restrict the ability of doctors, nurses and other providers to share information needed to treat their patients. In other situations, though, personal health information generally may not be used for purposes not related to health care, and covered entities may use or share only the minimum amount of protected information needed for a particular purpose. In addition, patients would have to sign a specific authorization before a covered entity could release their medical information to a life insurer, a bank, a marketing firm or another outside business for purposes not related to their health care.
- **Prohibition on Marketing.** The final privacy rule sets new restrictions and limits on the use of patient information for marketing purposes. Pharmacies, health plans and other covered entities must first obtain an individual's specific authorization before disclosing their patient information for marketing. At the same time, the rule permits doctors and other covered entities to communicate freely with patients about treatment options and other health-related information, including disease-management programs.
- **Stronger State Laws.** The new federal privacy standards do not affect state laws that provide additional privacy protections for patients. The confidentiality protections are cumulative; the privacy rule will set a national "floor" of privacy standards that protect all Americans, and any state law providing additional protections would continue to apply. When a state law requires a certain disclosure -- such as reporting an infectious disease outbreak to the public health authorities -- the federal privacy regulations would not preempt the state law.
- **Confidential communications.** Under the privacy rule, patients can request that their doctors, health plans and other covered entities take reasonable steps to ensure that their communications with the patient are confidential. For example, a patient

could ask a doctor to call his or her office rather than home, and the doctor's office should comply with that request if it can be reasonably accommodated.

- Complaints. Consumers may file a formal complaint regarding the privacy practices of a covered health plan or provider. Such complaints can be made directly to the covered provider or health plan or to HHS' Office for Civil Rights (OCR), which is charged with investigating complaints and enforcing the privacy regulation. Information about filing complaints should be included in each covered entity's notice of privacy practices. Consumers can find out more information about filing a complaint at <http://www.hhs.gov/ocr/hipaa> or by calling (866) 627-7748.

HEALTH PLANS AND PROVIDERS

The privacy rule requires health plans, pharmacies, doctors and other covered entities to establish policies and procedures to protect the confidentiality of protected health information about their patients. These requirements are flexible and scalable to allow different covered entities to implement them as appropriate for their businesses or practices. Covered entities must provide all the protections for patients cited above, such as providing a notice of their privacy practices and limiting the use and disclosure of information as required under the rule. In addition, covered entities must take some additional steps to protect patient privacy:

· Written Privacy Procedures. The rule requires covered entities to have written privacy procedures, including a description of staff that has access to protected information, how it will be used and when it may be disclosed. Covered entities generally must take steps to ensure that any business associates who have access to protected information agree to the same limitations on the use and disclosure of that information.

- Employee Training and Privacy Officer. Covered entities must train their employees in their privacy procedures and must designate an individual to be responsible for ensuring the procedures are followed. If covered entities learn an employee failed to follow these procedures, they must take appropriate disciplinary action.
- Public Responsibilities. In limited circumstances, the final rule permits -- but does not require --covered entities to continue certain existing disclosures of health information 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 that involves limited data or has been independently approved by an Institutional Review Board or privacy board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security. The privacy rule generally establishes new safeguards and limits on these disclosures. Where no other law requires disclosures in these situations, covered entities may continue to use their professional judgment to decide whether to make such disclosures based on their own policies and ethical principles.
- Equivalent Requirements For Government. The provisions of the final rule generally apply equally to private sector and public sector covered entities. For example, private hospitals and government-run hospitals covered by the rule have to comply with the full range of requirements.
-

OUTREACH AND ENFORCEMENT

HHS' Office for Civil Rights (OCR) oversees and enforces the new federal privacy regulations. Led by OCR, HHS has issued extensive guidance and technical assistance materials to make it as easy as possible for covered entities to comply with the new requirements. Key elements of OCR's outreach and enforcement efforts include:

- Guidance and technical assistance materials. HHS has issued extensive guidance and technical materials to explain the privacy rule, including an extensive, searchable collection of frequently asked questions that address major aspects of the rule. HHS will continue to expand and update these materials to further assist covered entities in complying. These materials are available at <http://www.hhs.gov/ocr/hipaa/assist.html>.
- Conferences and seminars. HHS has participated in hundreds of conferences, trade association meetings and conference calls to explain and clarify the provisions of the privacy regulation. These included a series of regional conferences sponsored by HHS, as well as many held by professional associations and trade groups. HHS will continue these outreach efforts to encourage compliance with the privacy requirements.
- Information line. To help covered entities find out information about the privacy regulation and other administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, OCR and HHS' Centers for Medicare & Medicaid Services have established a toll-free information line. The number is (866) 627-7748.
- Complaint investigations. Enforcement will be primarily complaint-driven. OCR will investigate complaints and work to make sure that consumers receive the privacy rights and protections required under the new regulations. When appropriate, OCR can impose civil monetary penalties for violations of the privacy rule provisions. Potential criminal violations of the law would be referred to the U.S. Department of Justice for further investigation and appropriate action.
- Civil and Criminal Penalties. Congress provided civil and criminal penalties for covered entities that misuse personal health information. For civil violations of the standards, OCR may impose monetary penalties up to \$100 per violation, up to \$25,000 per year, for each requirement or prohibition violated. Criminal penalties apply for certain actions such as knowingly obtaining protected health information in violation of the law. Criminal penalties can range up to \$50,000 and one year in prison for certain offenses; up to \$100,000 and up to five years in prison if the offenses are committed under "false pretenses"; and up to \$250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.