HIPAA Privacy and Security Implications for Field Triage

Roslyne Schulman

ABSTRACT

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 addresses insurance reforms, medical savings accounts, fraud and abuse provisions, and health information standards. This report discusses HIPAA issues that could impact field triage and emergency medical services.

Key words: triage; emergency medical services; trauma center; HIPAA.

PREHOSPITAL EMERGENCY CARE 2006;10:1–3

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, addresses insurance reforms, medical savings accounts, fraud and abuse provisions, and health information standards.

HIPAA's health information standards apply to "covered entities": health plans, health care clearinghouses (e.g., billing services), and providers who transmit health information electronically using certain standard transactions (claims, benefit eligibility, and so on). Providers transmitting health information that are covered entities include hospitals, doctors, pharmacies, trauma centers, and maybe emergency medical services (EMS) (if they bill). The health information standards probably do not apply to 9-1-1 call centers.

Privacy

The privacy goal of HIPAA is the protection of individually identifiable health information, also known as "protected health information." Essentially this is information that connects an individual with his or her health status, condition, or treatment. The deadline for compliance with HIPAA Privacy Rules was April 14, 2003.

The basic principle under the Privacy Rule is that absent a written authorization from the individual to whom the information pertains, a covered entity may not use or disclose protected health information except as the Privacy Rule permits or requires. Under the Privacy Rule, a covered entity is permitted to use and disclose private health information without an individual's authorization for the following purposes or situations:

- To the individual
- For treatment, payment, and health care operations
- In response to an inquiry about the patient by name when the patient has not objected to the inclusion of the information—name, general description of the patient's condition, and location within the facility—in the hospital's patient directory
- Incident to an otherwise permitted use/disclosure
- As required or permitted by law, including for certain public interest and benefit activities
- Under a data use agreement, a "limited data set" may be used/disclosed for research, public health, or health care operations
- For general research if the requirement to obtain patient authorization has been properly waived by a privacy board or institutional review board.

Although generally a covered entity must obtain an individual's written authorization for use of disclosure of protected health information, protected health information may be disclosed without authorization for treatment, payment, or health care operations even if disclosure is made to a provider who is not a covered entity as defined previously.

HIPAA's limitations on uses and disclosures of protected health information have specific implications for field triage. The exchange of protected health information in making triage determinations is considered "treatment" and would be exempt from the requirement for patient authorization. Additionally, as a permitted disclosure for payment purposes, hospital emergency departments and trauma centers may give a patient's payment information to the EMS provider who transported the patient for billing purposes.

In an emergency situation or in the case of patient incapacity, a covered entity may disclose private health information such as the patient's location, general condition, or death for notification purposes when it is in the best interest of the patient. For example, a covered entity may ask police for help in locating and communicating with the family if the patient is injured or dead.

HIPAA limits the use and disclosure of private health information to the "minimum necessary." A covered entity must make reasonable efforts to use, disclose, and request only the "minimum necessary" protected health information needed to accomplish the intended purpose. However, the "minimum necessary" requirement does not apply to a disclosure or request by a health care provider for treatment. Also,

From the American Hospital Association, Washington, DC.

Address correspondence to: Roslyne Schulman, American Hospital Association, Liberty Place, Suite 700, 325 Seventh Street, NW, Washington, DC 20004-2802. e-mail: <rschulman@aha.org>.

doi:10.1080/10903120600728771

there is no "minimum necessary" requirement when the disclosure is to the individual who is the subject of the protected health information or his or her personal representative.

A covered entity must provide to a patient a notice of its privacy practices describing how it will use and disclose protected health information as well as the patient's rights in relation to his or her information. The covered entity also is required to use reasonable efforts to have the patient acknowledge receipt of the notice of privacy practices. In an emergency, the distribution of the notice must occur "as soon as practicable after." An acknowledgement of notice receipt is not required in an emergency.

HIPAA's administrative requirements are meant to be flexible and scalable to the size and complexity of the specific covered entity. These requirements include privacy policies and procedures, privacy personnel, workforce training and management, mitigation, data safeguards, complaints, retaliation and waiver, and documentation and record retention.

In general, the HIPAA Privacy Rule preempts state privacy laws that are contrary. Exceptions to this preemption rule include laws that require greater protection of private health information, certain reporting requirements (e.g., disease or injury, child abuse, and so on), and health plan reporting. The Secretary of the Department of Health and Human Services (HHS) may allow other exceptions to preempting contrary state law in certain circumstances (e.g., an exception necessary for compelling public health reason). To date, the Secretary has granted no exceptions.

Enforcement of the HIPAA Privacy Rules currently is complaint driven. Civil monetary penalties are $100 per failure, not to exceed $25,000 per year for multiple violations of an identical requirement, and HHS has recently finalized a single civil enforcement rule applicable to all aspects of HIPAA. Criminal penalties are imposed and enforced by the Department of Justice for the following: "knowingly obtains or discloses" private health information in violation of HIPAA. Fines are up to $50,000 and up to one year in prison if wrongful conduct involves "false pretenses." If the violation involves intent to sell, transfer, or use private health information for commercial advantage, personal gain, or malicious harm, fines are up to $250,000 and up to ten years in prison.

Security

The intent of the security provisions of HIPAA is to establish a framework and infrastructure to support the privacy and confidentiality of a patient's medical information by creating standards that ensure the integrity and availability of health information and protect against unauthorized access or transmission. The final Security Rule was published February 20, 2003, and compliance was required by April 21, 2005.

The HIPAA Privacy Rule described previously covers what information needs to be protected and how that information may be used and disclosed. HIPAA Security Rules establish administrative, physical, and technical safeguards to protect the information.

Generally, the HIPAA security requirements ensure confidentiality (who can see the information), integrity (the information has not been altered inappropriately), and availability (it can be accessed on a timely basis by authorized users) of information. The requirements apply only to electronic protected health information, whereas the Privacy Rule extends to oral and written communications. The Security Rule's requirements apply to the electronic protected health information that a covered entity creates, maintains, and transmits. Under the Security Rule, covered entities must protect against reasonably anticipated threats or hazards to the security or integrity of the information, protect against reasonably anticipated uses and disclosures as outlined in the Privacy Rule, ensure compliance by workforce, and develop business associate contracts as appropriate.

Implementation of the security regulations also is meant to be scalable and flexible. Individual organizational approaches may account for size, complexity, technical infrastructure, cost, and the potential security risks the organization actually faces. The security regulations establish administrative, physical, and technical standards for implementation. Within each standard are a series of implementation specifications that can be either required or addressable. In this context, required is a "must" and organizations must implement the specifications. For addressable implementation specifications, the covered entity, after risk analysis, may implement the specification if it is reasonable and appropriate; implement an equivalent measure, if that is reasonable and appropriate; or not implement the specifications if it is not reasonable and appropriate.

The HIPAA Security Administrative Standards include standards for security management (risk analysis and risk management), assigned responsibility to a single point of contact, and workforce security (termination procedures and clearance procedures). They also include standards for information access management, security awareness and training, security incident procedures, a contingency plan for disaster recovery, evaluation, and business associate contracts.

The HIPAA Security Physical Standards are facility access controls, workstation use, workstation security, and device and media controls. HIPAA Security Technical Standards are written for access control (unique user ID, emergency access, automatic logoff, and encryption and decryption), audit controls, integrity, person or entity authentication, and transmission security.

Like the Privacy Rule, the HIPAA Security Rule has implications for field triage. Trauma centers and even EMS systems (if they bill) would be covered entities subject to the requirements of the Security Rule. As covered entities, they must establish proper administrative policies and procedures, implement appropriate technical safeguards, and acquire necessary security equipment and technology to meet the rule's requirements, if they have not done so already. This may necessitate new purchases, expansions, and upgrades. It also will require an ongoing process of assessing threats and risks and determining appropriate actions to take to address identified threats and risks—a one-time assessment is not enough.

SUMMARY

Field triage engages EMS systems and trauma centers. HIPAA Privacy and Security Rules do apply to trauma centers and EMS systems (if they bill for their services).