HIPAA & Healthcare: A New Way of Sharing and Caring

By: Alan S. Goldberg
Gouston & Storrs
400 Atlantic Avenue
Boston, MA 02109
617.482.1776
Adjunct Professor of Law, Suffolk University Law School, Boston, MA
http://www.hipaahero.com (sm)
May 2, 2001

For healthcare providers and payors, HIPAA is a metaphor for a new way of sharing health information and caring about its creation, use and disclosure. Now in addition to quality of care, the quality of privacy, confidentiality and security of health information will be a primary feature of how hospitals and health systems providers, do business every day.

For many years, there have been many federal and state laws which have not gotten a lot of attention, and which provide many privacy protections to hospital patients and their families. Before HIPAA, traditional practices have emphasized openness rather than the hiding of information, and now hospitals, payors, and health systems will have to change the way they do business in order to increase privacy protections. Somewhat surprisingly, hospitals have in

general remained wide open to visitors, patient advocates, and others on a round-the-clock basis and without nurses' stations or other health information areas becoming high security zones. This means that for hospitals, the security challenges are far greater than ever.

When Congress enacted the Health Insurance Portability and Accountability Act of 1996, commonly known as "HIPAA", changes in healthcare delivery began that eventually will be as great as those made by the Medicare and Medicaid programs, the imposition of anti-kickback prohibitions, and the change to prospective payment. In addition, the publicity being given to the significance of privacy protections and the Internet, banking and other financial institutions, and the federal and state governments, has caught the attention of the public and the media, with healthcare privacy taking center stage as an expected and demanded right and entitlement. Paying for it, however is, as usual, quite another thing all together. But that doesn't matter, because HIPAA contains no dispensations for those not having the funds to support HIPAA consistency.

HIPAA provides for new and complex standards relating to health information security, the adoption of code sets for standard transactions, and the maintenance of privacy and confidentiality of individually identifiable health information. The HIPAA protections are in a proposed security and electronic signature standards rule issued August 12, 1998 providing for many new security features; in a final rule issued August 17, 2000 and setting forth eight of what ultimately will be ten or more standards for electronic transactions and

codes relating to health claims, healthcare payments and remittance advices, and the like; and in a final privacy rule which, including the Preamble, is over 1,500 pages and is even larger than Senator Hillary Clinton's 1,400 pages or so that were intended to cause the entire healthcare delivery system to be changed radically.

Privacy under HIPAA is special because Congress, was given an opportunity to pass a new law to protect healthcare privacy. Because Congress did not act in time, HHS on November 3, 1999 issued a proposed rule and on December 28, 2000 issued a final rule, to provide standards for privacy of individually identifiable health information. The privacy rule creates a framework for ensuring the safety, security and integrity of electronically stored and transmitted healthcare information, as well as healthcare information in paper form or communicated verbally.

Based upon the final rules already issues, hospitals and most health plans are going to be directly affected by the HIPAA privacy rule -- a covered entity being the descriptive term used -- if, at any time, health information in electronic form is transmitted by the hospital or health plan in connection with one of the ten covered transactions. In addition, hospitals with which protected health information is shared by other healthcare providers and by health plans who are covered by HIPAA, can be subject to the business associates part of the final privacy rule. And if the final security rule looks like the proposed versions, hospitals will be required to observe new and strict standards regarding how health information is dealt with in electronic format.

Even more important, though, is the paradigm shift: regardless of what happens to the HIPAA rules, patients, families, and advocates are going to continue to read state and federal privacy laws in addition to HIPAA, and consumer protection laws and state constitutions, as the privacy issue continues to attract attention and gets media publicity. So, the sooner providers realize that the era of openness is over and the era of privacy protection, including but not only relating to HIPAA, is here forever, the better.

The penalties for ignoring all of this will be great, because of monetary sanctions and possible jail time, and lost marketing opportunities as the customers (some still call them patients, but their patience is being tried like never before) demand what they now want (or are told they want) and those who cannot deliver it suffer. No one want to be the first convict who tells the story of having gotten the maximum sentence --ten years in jail -- by being a person who knowingly uses or causes to be used a unique health identifier; obtains individually identifiable health information relating to an individual; or discloses individually identifiable health information to another person, with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.

The words and phrases used in the proposed and final rules are sometimes clear, and sometimes not so clear. And sometimes, specific mention is made to reasonability of actions to be taken, and other times no such mention is made; “practicably”; “professional judgment”; “reasonable inferences”;

"satisfactory assurance"; "reasonable efforts"; "standards of ethical conduct"; "reasonably ensure"; "to the extent practicable"; a "reasonable time" and "reasonably designed" appear sometimes, but not other times, and "including" appears sometimes and "including, without limitation" appears other times. Sometimes there is a "must" and other times there is a "may." Somewhat surprising, however, is the exuberance shown in the Preamble to the final privacy rule about a "firewall" – there are too many mentions of firewalls to count all of them, and it seems like HHS really likes whatever it means by using that word, although the meaning is not always clear. And the HIPAA Preamble specifically disclaims any intention on the part of HHS to establish "best practices"; that will be left, it seems, to others.

With all of this in mind, more details follow; it's time to learn your HIPAA:

The HIPAA rules will affect most records relating to healthcare and just about every healthcare provider including hospitals, nursing homes, physicians, and managed care organizations, and payors, health plans, and healthcare clearinghouses (such as a service bureau that converts healthcare data from one format to another), as well as most who deal with them. The Medicare program and the Medicaid program, as administered by federal and state authorities, are affected by the HIPAA rules, as well.

The final electronic transactions and code sets rule adopts certain formats for transactions involving information exchanges to carry out financial or

administrative activities related to healthcare, including the following types of information exchanges: (1) healthcare claims or equivalent encounter information; (2) healthcare payment and remittance advice; (3) coordination of benefits; (4) healthcare claim status; (5) enrollment and disenrollment in a health plan; (6) eligibility for a health plan; (7) health plan premium payments; (8) referral certification and authorization; (9) first report of injury; (10) health claims attachments; and (11) other transactions that HHS may prescribe by regulation.

Thus, if a hospital, as a covered entity, conducts with another covered entity (or within the same covered entity) such as a health plan, using electronic media, one of those transactions for which HHS has adopted a standard, the hospital must conduct the transaction as a standard transaction following the standards required by the final electronic transactions and codes rule.

When it comes to privacy, the focus of HIPAA is on the privacy and confidentiality of information (whether oral or recorded) that relates to any of the following: information, whether oral or recorded in any form or medium, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and 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. In other words, HIPAA protects health information maintained by hospitals for and about their patients.

The final privacy rule covers health plans and healthcare clearinghouses; and healthcare providers, such as hospitals, who transmit health information electronically in connection with HIPAA standard transactions. The privacy rule applies specifically to protected health information, which under the proposed privacy rule was defined to mean any individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity. But in the final privacy rule, protected health information also includes individually identifiable health information transmitted or maintained in any form other than in electronic media, and so information on paper and verbally transmitted will be protected as well.

A hospital or a health plan will be considered a covered entity and therefore directly affected by the final privacy rule if, at any time, health information in electronic form is transmitted by the hospital in connection with one of the covered transactions listed above. The final privacy rule establishes individual rights with respect to the covered health information, and requires hospitals and health plans to adopt safeguards to protect the confidentiality of protected health information against unauthorized use and disclosure.

Several big changes in doing business are required the final privacy rule. First of all, a covered entity is permitted to disclose protected health information about a patient to that particular patient; or in a manner permitted by a particular form of consent of a patient when using or disclosing inside the hospital; and in certain limited circumstances, without a patient's consent. Unlike the proposed privacy rule, the final privacy rule requires consent from a

patient even in order to carry out basic treatment, payment, or healthcare operations – consent is not presumed, except in certain limited circumstances including emergencies.

When using or disclosing protected health information, a covered entity will have to make reasonable efforts to limit information to the minimum necessary to do whatever the information is needed to do, and no more. But there is no minimum necessary requirement when it comes to disclosures to or requests by a healthcare provider for treatment of a patient, or in general as to disclosures of a patient's information to the patient. The choice as to how much protected health information to disclose will have to be based upon policies that are in place and that provide guidance regarding how information is to be disclosed and to whom, and the risk of mistake is a risk that the covered entity will be taking every day.

Another big change is that covered entities, which already will usually have contracts with those with which they deal, will be required to enter into written contracts with these business associates before protected healthcare information can be shared with them. The definition of business associates includes most consultants doing business with covered entities, such as those providing legal, actuarial, accounting, management, administrative, accreditation, or financial services. In addition, a covered entity may be a business associate of some other covered entity, and another covered entity may be a business associate of a covered entity.

The Preamble to the final privacy rule says that for compliance purposes, independent contractors are members of the workforce if no business associate contract exists. A business associate may not, at the same time, be a member of the covered entity's workforce, so someone will have to decide whether independent contractors are members of the workforce or business associates. This is an important issue because members of the workforce would seem to be subject to the HIPAA penalties, unlike business associates which HHS has no direct authority under HIPAA to penalize. Still left unclear is whether members of the board of directors of healthcare providers are or should be considered to be either members of the workforce or business associates.

The final privacy rule requires these contracts to include provisions dealing with permitted and required uses and disclosures of information by the business associate; the use by the business associate of safeguards to protect information; making business associate internal practices, books, and records available to HHS for determining the covered entity's compliance with the final privacy rule; and requiring the return or destruction of protected health information. And if the business associate hires others who will receive protected health information, they must also protect the information in the same way as the business associate.

In general, the final privacy rule will require covered entities to obtain a patient's explicit authorization before disclosing protected health information to those outside of the facility. The conditions governing the authorization differ depending on the situation involved, and patient can revoke authorizations.

Someone from outside of the covered entity who asks for a use or disclosure would submit an authorization form to the covered entity. The form would have to: (1) describe the information to be used or disclosed; (2) name the person to be authorized to make the use or disclosure and the person to whom the requested use or disclosure will be made; (3) have an expiration date; (4) confirm the patient's right to revoke the authorization; (5) warn the patient that redisclosed information may not necessarily continue to be protected; (6) be signed by the patient; and (7) be in plain language (note that the model form set forth at the end of the proposed privacy rule has been eliminated in the final privacy rule).

The final privacy rule would establish federal protection of the following basic rights for protected health information, with notice of them to be given in plain language: (1) the right to notice of the uses and disclosures of protected health information that may be made by the covered entity, and patients' rights and the covered entity's legal duties with respect to protected health information, (2) the right to obtain access to protected health information, (3) the right to receive an accounting of how a patient's protected health information has been disclosed, and (4) the right to request changes in protected health information that is inaccurate or incomplete.

Agreeing to more limits on uses or disclosures would be optional on the part of a covered entity, but once an agreement is reached with the patient, it would be binding on the covered entity.

Covered entities will be required to update their notices when they make a material changes in uses and disclosures, patients' rights, the covered entity's duties, or other privacy practices originally set forth in the notice. In addition, a covered entity that maintains a web site providing information about the covered entity's services or benefits will have to prominently post its notice on its web site and make the notice available electronically through the web site.

In addition to having access to their own protected health information, patients will also have a right of access to their protected health information maintained by a business associate of the covered entity. Denial of a patient's request to inspect or copy his or her own protected health information would be permitted only under very limited circumstances.

The final privacy rule also contains special provisions that give family members, other relatives, or close personal friends of a patient, or any other person that the patient designates, protected health information directly relevant to the healthcare or payment related to the healthcare for the patient. Certain notifications to family members, personal representatives, and others responsible for the patient's care about location, general condition, and death, are also permitted. Note that protected health information continues to be protected even after the death of a patient, and the deceased patients rights will be inherited by an executor, administrator, or other personal representative of the patient's estate.

There is also a special exception to permit disclosures by covered entities to funeral directors in anticipation of or after a patient's death. The funeral director lobby is, indeed, powerful.

In order to protect protected health information from inappropriate use or disclosure, covered entities will be required to have many new policies and procedures, and to have a privacy official and person responsible for receiving complaints. A HIPAA training program will also be needed, which wise covered entity administrators will complement with a HIPAA corporate compliance program meeting Department of Justice Federal Sentencing Guidelines requirements. And in anticipation of the final security rule, a covered entity will need appropriate administrative and physical safeguards to protect the privacy of protected health information that is in electronic form.

The final privacy rule also contains a provision for the de-identification of protected health information. Covered entities would be permitted to strip identifiers from healthcare information and use and disclose such de-identified information, subject to certain conditions.

With respect to security standards, HHS will adopt those proposed by healthcare industry and other groups instead of HHS coming up with its own standards. HHS researched marketplace security standards to develop the security standards proposed to be adopted in the security rule in order to safeguard protected health information. These security standards would not require covered entities to use particular technologies or particular hardware or

software. Instead, covered entities that electronically store and transmit healthcare information would have to comply with certain minimum threshold protocols and procedures in four basic categories, in whatever manner is consistent with the HIPAA requirements.

The categories involve various aspects of ensuring the integrity, confidentiality and availability of electronically stored and transmitted healthcare 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.

HHS comments to the proposed security rule indicate that HHS would require every aspect of compliance with these four categories to be documented, monitored, reviewed and regularly updated. So, for covered entities, some things never change: document, document and document, will continue to be the rule.

The proposed security rule would create twelve categories for policies and procedures, including: (1) certification of data systems to evaluate compliance with security standards (with third-party certification likely to be mandated), (2) "chain of trust" agreements among the regulated entity and each other entity with which health care information is exchanged, (3) a contingency plan to ensure continuity and preservation of data in emergency situations, (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 healthcare information, (8) security configuration management procedures to coordinate overall security including documentation, hardware and software systems review, and virus checking, (9) protocols for reporting and responding to security breaches, (10) establishment of a security management structure with 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.

In addition, the proposed security rule would impose requirements relating to the physical protection of data systems and data from intrusion and from environmental hazards. This will require the: (1) formal assignment security responsibility to a responsible person or entity, (2) development of controls on access to and the physical manipulation of hardware components such as disks, keyboards and monitors, (3) development of disaster and intrusion response and recovery plans, (4) implementation of personnel identification verification procedures for physical access to data sites, (5) retention of maintenance records (6) enforcement of security clearances hierarchies on a "need-to-know" basis, and (7) implementation of detailed protocols regarding activities and security at the work station level.

Requirements relating to software controls and protocols within and surrounding particular data systems would also be imposed under the proposed security rule, in order to: (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.

Finally, the proposed security rule would impose requirements relating to software controls and protocols incident to electronic storage and transmission of healthcare 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 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 encryption techniques are not used to control transmission of information, HHS would also require (1) alarms to signal abnormal communication conditions, (2) automatic recording of audit trail information, and (3) a means of entity authentication.

One of many challenges that covered entities face in understanding HIPAA rules is the question, time and again, that will have to be asked: is a particular state law contrary to HIPAA or more stringent than HIPAA – this is the issue popularly known as "preemption". Some felt that HIPAA should be the only privacy law affecting healthcare and that state laws that are contrary

should fall by the wayside. Instead, states are permitted to have laws that are more stringent than HIPAA. Because so many state privacy laws already exist and some will not clearly indicate whether they should be considered contrary or more stringent, each covered entity will have to relearn the state privacy law for the state in which it is located, and perhaps the law of other states as well. Sadly, all of this can lead to states of confusion, as the definitions in the final privacy rule are parsed through and compared.

HIPAA grants HHS the authority to impose civil monetary penalties against covered entities which fail to comply with the requirements of the final rules, and also establishes criminal penalties for certain wrongful disclosures of protected health information. This authority has been delegated to the Office of Civil Rights of HHS, which will issue rules to indicate how enforcement will occur. HIPAA does not provide for a private right of action for patient. But under state law patients might be considered third party beneficiaries of contracts with business associates, which could form the basis for a claim against the covered entity and its business associate under the contract, and state consumer protection law could also provide a basis for a patient to seek to enforce privacy rights in reliance on the HIPAA final rules as analogous and persuasive standards.

In addition to being punished by the Office for Civil Rights, to which HHS has delegated enforcement responsibility, covered entities will have to develop their own internal system of sanctions for employees and business associates who violate the covered entity's policies, including termination of employment

and termination of business associate contracts. And it can be expected that surveyors under the Medicare and Medicaid programs eventually will add HIPAA-related deficiencies to those already available for assessment, and that accrediting organizations will add HIPAA compliance to their lists of areas of focus.

Fortunately, HHS has taken the position that the sanctions, while already set forth in HIPAA, are not going to be enforced until an enforcement date in or about April 2003 for most entities affected by HIPAA 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 healthcare 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."

Until the Office for Civil Rights provides rules regarding penalties, we will not know how the penalties process will work. Whether only covered entity organizations will be penalized for violations of HIPAA, or whether in some instances members of the workforce will be penalized, should become clear when more rules are issued. It should also be borne in mind that these direct

HIPAA penalties are in addition to any that others might try to impose against employees or business associates under state laws that might apply to a violation, including laws that license professionals who work in covered entities and laws permitting patients and families to sue for damages if someone is hurt because of a privacy violation. This means that wise covered entity operators, in addition to learning HIPAA, are talking to their insurance agents and advisors about how best to maintain the proper coverages and limits in order to get the most cost-effective protection. And consideration should also be given to how accountants are going to deal with HIPAA in their financial reports and audit certifications.

Healthcare will never be the same when HIPAA Administrative Simplification provisions take effect. Because we are all patients some time or another, we all will be affected in one way or another, as will just about every covered entity and health system and everyone who works in or with them. Hopefully, Administrative Simplification will not get in the way of the timely and efficient provision of healthcare, which should be the overriding goal of any healthcare delivery system. We will just have to wait and see how all of this works out.

But now, it's late and therefore it's time to get going and learn the new rules. Remember, you never want to be behind a HIPAA.

ASG/tt

[The author acknowledges with appreciate the contribution of his colleagues at Goulston & Storrs, Boston, to this paper -- each and every one is a HIPAA HERO (sm); the strengths of this paper are theirs, the inadequacies are the author's.]