HIPAA Compliance: The Law Reality, and Recommendations

Michael Schoppmann, JD

The physicians of today and tomorrow face the most daunting set of regulations ever imposed on the practice of medicine. Through the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal government has thrust its regulatory authority into three of the most controversial and cutting-edge in medical practice management: privacy, electronic transactions, and security. Through practical insights, the authors' goal is to introduce physicians to HIPAA’s basic tenet’s, the evolutionary nature of the regulations, and the concept that they can manage HIPAA without bankrupting their practices or sealing themselves away from their patients.

Key Words: HIPAA, privacy, security, compliance

INTRODUCTION

The roller-coaster ride of speculative highs and reality lows in the implementation of the federal Standards for Privacy of Individually Identifiable Health Information (privacy standards) [1] has come to a tormented end. The controversial standards, mandated by the health Insurance Portability and Accountability Act of 1996 (HIPAA) [2] and adopted by the U.S. Department of Health and Human Services (HHS), are here (enforcement began April 14, 2003), and medicine is forever and inextricably altered. What perhaps is the threshold (and preeminent) requirement for every physician or practice seeking to manage the requirements of the privacy standards is the recognition that these regulations have undergone significant changes over the past 3 years; they will continue to undergo modification; and they can be managed without the need to undertake unrealistic, economically unfeasible, and wholly unnecessary changes to the practice of medicine.

REALITY AND RECOMMENDATIONS

Physicians should take a collective deep breath, throw out all of the misinformation they have been fed over the past several years about the privacy standards, and realize three simple facts. First, regardless of the fully justified frustrations of every aspect of medicine, HIPAA is here to stay. Second, the present version of the collective HIPAA regulations (especially the privacy standards) bears little resemblance to those generated by the original set that caused such hysteria almost 3 years ago. Third, physicians can manage these regulations.

MORE THAN JUST PRIVACY

Most physicians are aware that HIPAA addresses more than just the privacy of individually identifiable health information but contains multiple components, the three major components being the privacy standards, transactions and code set standards (relating to the electronic filing of claims and other electronic transactions), and standards for the security of health information (the “administrative simplification” provisions of HIPAA are set forth in Title II, Subtitle F of HIPAA [3]). HIPAA also mandates unique identifiers for health plans, health care providers, employers, and individuals [4]. A rule adopted January 23, 2004, and effective May 23, 2005, adopts the National Provider Identifier as the standard unique health identifier for health care providers. When the National Provider Identifier is implemented, entities covered by HIPAA will use only the national Provider Identifier to identify health care providers in all standard transactions. [5].

PRIVACY STANDARDS

By way of background, the privacy standards are applicable to health plans, health care clearinghouses, and those health care providers that conduct certain financial and administrative transactions electronically (“covered entities”) and address the privacy of individually identifiable health information created or received by a covered entity (“protected health information” [PHI]) [6]. In basic, terms, they define the circumstances in which an entity may use and disclose PHI; establish individual rights with respect to the information; and require covered entities to adopt safeguards to protect the confidentiality of the information, with civil and criminal penalties for noncompliance [7]. The privacy standards took effect on April 14, 2001. Most covered entities were to have complied with the privacy rules by April 14, 2003, though small health plans had until April 14, 2004, to comply. [8].

Although originally an unworkable set of non-reality-based regulations, the privacy standards underwent a deconstructive process over the 2 years after adoption [9].
Through the ongoing issuance of “guidance” and modifications, HHS sought, and continues to seek, to distance itself from the original (and completely unworkable) version of HIPAA [10]. The goal of these modifications and guidelines, as cited by his HHS secretary Tommy Thompson, is to “make sure patients receive the highest quality care and begin the process of issuing guidelines on how this rule should be implemented” [11]. Thompson says such guidelines will allow the clarification of some of the confusion regarding the impact the rule might have on health care delivery and access. Moreover, HHS will consider the issuance of future modifications “as necessary” to ensure that the quality of care does not suffer inadvertently from the rule [11].

Through the issuance of such guidelines or modifications, HHS has stated that it seeks to ensure that doctors and hospitals will have access to necessary medical information about patients they are treating and will be able to consult with other physicians and specialists regarding patient care; patient care will be delivered in a timely and efficient manner and not unduly hampered by the confusing requirements surrounding consent forms; and parents will have access to information about the health and well-being of their children, including information about mental health, substance abuse, or abortion [11].

One way HHS’s Office for civil Rights, the enforcement agency for the privacy standards, seeks to modify or at least clarify confusing and ambiguous provisions of the privacy standards is by posting on its Web site its answers to frequently asked questions submitted to the office, as well as a multitude of other documents and guidance on the implementation of the privacy standards [10].

PREEMPTION ISSUES

Of note is that the HIPAA standards, although not inherently preemptive of more stringent state laws, may pose complex questions as to their interplay, or potential conflict, with state laws [12]. Moreover, the privacy standards do not preempt other federal laws and/or rules that provide greater privacy of PHI than the privacy standards themselves [13]. As a result, physicians seeking to achieve privacy compliance must analyze their practices from a threefold prospective- directed at the federal privacy standards, other federal laws and rules affecting the privacy standards, other federal laws and rules affecting the privacy of health care information., and the potentially unique requirements of any present or future state laws or rules that relate to the privacy of health care information. Many states have worked toward designing rules to establish uniform health care enrollment and claim forms and requiring that health care payers and providers, and their agents and vendors, comply with privacy requirements (see, e.g., the Health Information Electronic Data Interchange Technology Act [14], the North Carolina Insurance Information and Privacy Act [15], and the Confidentiality of Medical Information Act [16]; for additional information on state privacy laws and regulations, see the Web site of Georgetown University’s Institute for Health Care Research and Policy, Health Privacy Project [17])

CONTINUING REQUIREMENTS

In practical terms, Physician practices already should have taken specific steps and developed policies and procedures to comply with the privacy standards, implementing at least the following requirements [18]:

• designating a “privacy officer” responsible for the development and implementation of privacy policies and procedures;
• safeguarding and limiting access to PHI;
• training staff members on privacy rules;
• establishing and imposing sanctions for staff members who break the rules;
• maintaining a log of certain disclosure;
• adopting a complaint process that identifies a contact person for complaints;
• developing procedures to permit individuals to inspect, copy, and/or amend their own records;
• furnishing patient with a notice of privacy practices and patients’ rights; and
• executing or revising contracts with business associates to obtain assurance of their compliance with the regulations.

REALITY AND RECOMMENDATIONS

The HIPAA privacy standards do not require that physicians seal themselves in locked rooms to discuss patients’ health information. They do require that physicians, and their medical practices, take “reasonable measures” to protect personal health information. In fact, it is recognized by HHS that unanticipated disclosures will occur, and those practices that had in fact developed and complied with their own “reasonable measures” will hold an immediate defense to any investigation or complaint [19]. In seeking to build such “reasonable measures,” physicians have enormous resources available to them, most of them free of charge, from their professional associations, specialty societies, malpractice insurers, and a host of other reputable entities.

Through the mechanism of issuing ongoing “modifications” HHS has also been able to address a number of concepts as it develops them, while making significant changes to existing rules [20]. In the arena of privacy, some examples follow.

Marketing

The final version of the privacy standards requires a covered entity to obtain an individual’s prior written authorization to use his or her PHI for marketing purposes,
except for a face-to-face encounter or a communication involving a promotional gift of nominal value. HHS defines marketing to distinguish between the types of communications that are and are not marketing and makes it clear that a covered entity is prohibited from selling lists of patients and enrollees to third parties or from disclosing PHI to a third party for the marketing activities of the third party without the individual’s authorization. Doctors communicating with patients about treatment options or the covered entity’s own health-related products and services are not considered marketing.

Notice

The privacy standards require covered entities to provide patients with notice of the patient’s privacy rights and the privacy practices of the covered entity. The strengthened notice requires direct treatment providers to make a good faith effort to obtain a patient’s written acknowledgement of the notice of privacy rights.

Uses and Disclosures Regarding U.S. Food and Drug Administration (FDA)-Regulated Products and Activities

The final privacy standards permit covered entities to disclose PHI without authorization to a person subject to the jurisdiction of the FDA, for public health purposes related to the quality, safety or effectiveness of the FDA-regulated products or activities, such as collecting or reporting adverse events, dangerous products, and defects or problems with FDA-regulated products.

Incidental Use and Disclosure

The final privacy standards acknowledge that uses or disclosures that are incidental to an otherwise permitted use or disclosure may occur. Such incidental uses or disclosure are not considered a violation provided that the covered entity has met the reasonable safeguards and minimum necessary requirements. For example, if these requirements are met, doctors’ offices may use waiting room sign-in sheets, hospitals may keep patients’ charts at bedside, doctors can talk to patients in semiprivate rooms, and doctors can confer at nurses’ stations without fear of violating the rule if overhead by a passerby.

Authorization

Patients will have to grant permission in advance for each type of nonroutine use or disclosure, but providers will not have to use different types of authorization forms.

Minimum Necessary

The final privacy standards exempt from the “minimum necessary requirement” any uses or disclosures for which the covered entity has received an authorization. Minimum necessary requirements are still in effect to ensure an individual’s privacy for most other uses and disclosure’s, including those necessary workers’ compensation programs.

Parents and Minors

The final privacy standards clarify that state law, or other applicable law, governs in the area of parents and minors. Generally, the privacy standards provide parents with rights to control the health information about their minor children, with limited exceptions that are based on state or other applicable law and professional practice. For example, where a state has explicitly addressed disclosure of a minor’s health information to a parent, or access to a child’s medical record by a parent, the final rules clarify that state law governs. In addition, the final rule clarifies that in the special cases in which the minor controls his or her own health information under such law and that law does not define the parents’ ability to access the child’s health information, a licensed health care provider continues to be able to exercise discretion to grant or deny such access, as long as that decision is consistent with the state or other applicable law.

Research

The final privacy standards allow researchers to use a single combined form to obtain informed consent for the research and authorization to use or disclose PHI for such research.

Limited Data Set

The final privacy standards permit the creation and dissemination of a “limited data set” (that does not include directly identifiable information) for research, public health, and health care operations. In addition, to further protect privacy, the final rules condition disclosure of the limited data set on a covered entity and the recipient entering into a “data use agreement.”

Looking ahead, HHS will continue to issue “guidance” to physicians in an ongoing attempt to answer common questions and clarify certain provisions of the HIPAA regulations through the web site of the Office for Civil Rights. Further clarification will be forthcoming in lawsuits that will test the privacy waters in the context of malpractice litigation, familial disputes, and government access to private medical records (see, e.g., Harmon v. Texas [21], the release of blood alcohol test results is permissible under HIPAA when disclosure is for law enforcement purposes and is pursuant to grand jury subpoena; United States ex rel. Stewart v. The Louisiana Clinic [22]. HIPAA preempts state law on the disclosure of patient information).

ELECTRONIC TRANSACTIONS
The second main component of HIPAA, addressing the setting of standards for electronic health care transaction (Table 1) and code sets [23] (see Social Security Act [24]; the transaction standards are established by the HIPAA Transaction Rule [25]), was originally set to take effect on October 16, 2002. However, H.R. 3323, the Administrative Simplification Compliance Act (ASCA), signed into law by President Bush on December 27, 2001, altered the timetable for compliance with the transactions and code set standards [26]. (The ASCA did not, however, affect the April 14, 2003, date for the implementation of the privacy standards [27].) The legislation provided that an entity that had not come into compliance with the transactions and code set standards by the October 2002 deadline could have received an extension of time for compliance until October 16, 2002, demonstrating how it would come into compliance over the following year [28].

To provide a disincentive to maintaining (or returning) to paper claims, the ASCA requires covered entities to submit HIPAA-complaint electronic Medicare claims to the Centers for Medicare and Medicaid Services (CMS) as a condition of payment [29]. The ASCA does provide an exception to the electronic filing requirement when no method other than written submission of claims is available and for “small providers” (defined as having fewer than 10 full-time-equivalent employees for physician practices) [30].

By now, practices should be compliant, if not near compliant, with electronic transaction standards. Although CMS provided more time after October 16, 2003, to come into compliance, that “contingency plan” will eventually come to an end. In February 2004, CMS announced its latest step toward ending the contingency plan for incoming Medicare claims. Effective July 1, 2004, CMS continued to allow the submission of noncompliant electronic claims, but the payment of such noncompliant claims will take an additional 13 days, that is, 27 days after the date of receipt [31].

SECURITY STANDARDS

The third component of HIPAA, the security standards [32], seeks to protect the security of health information in electronic form (both stored and transmitted), as opposed to the privacy standards, which apply to PHI in all forms—written, oral, and electronic. The security standards adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic PHI. The final rules were published on February 20, 2003. However, the deadline for compliance by health care providers is April 20, 2005 [33].

Security is designed to address safeguards and set uniform, minimum standards for such “electronic” issues as

- access authorization;
- encryption and decryption;
- data backup and storage;
- disaster recovery plans;
- contingency operations;
- maintenance records;
- security reminders;
- password management;
- workforce security;
- termination procedures, and
- safe disposal.

Some of this terminology should sound familiar, and radiology practices that have done their job implementing the privacy standards will be ahead of the security game because the privacy standards already require that a covered entity have in place “appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information” [34].

Fortunately, the final security standards provide for flexibility and “scalability” in meeting the requirements of the rule. There are multiple standards—general requirements that must be complied with— and some standards are to be implemented by a set of specifications, some of which are “required” and some of which are “addressable” [35]. Each required specification must be implemented as specified. Each addressable specification must be “addressed” to determine whether that particular specification is a reasonable safeguard for the practice to implement [36]. If it is reasonable, then the practice can either implement it as specified or decide to implement an “equivalent alternative measure.” If the decision is that the specification is inapplicable to the practice, that is, does not make sense to implement, and no alternative measure is needed to meet the required standard, the practice can determine not to implement that specification. Practices should keep in mind that the “addressable” specifications are not “optional” specifications; they must be addressed.

Compliance with the security standards starts, then, with a risk of assessment, using the standards and specifications of the security standards as the guide, followed by decision making and implementation. The decision making should be supported by considerations of probable risks, consequences, practice size and resources, technical capability, and the costs of implementing the possible security solutions [36]. Most radiology practices, particularly larger ones, have already dealt with security risks and resolutions surrounding the utilization of technology in the medical practice and the protection of health information. As with the privacy standards, however, much of compliance with the security standards is administrative, not technical. It is mandatory, then, that the risk assessment, the decision-making process, and the implementation of the methods for complying with the multiple specifications of the security standards are documented.

REALITY AND RECOMMENDATIONS

Physicians will not have to now become computer technicians, nor will their office staffs be forced to build information technology departments to cope with the security provisions of HIPAA. Rather, most medical practices, if not nearly all, have used, or use on an
ongoing basis, outside vendors for computer services. Physicians should now insist that any computer vendor they retain provide the medical practice with a “certificate of HIPAA compliance” attesting to the fact that they have brought the practice into compliance with the technical requirements of the HIPAA security regulations.

**COMBINED COMPLIANCE**

In consideration of the close interplay of the HIPAA privacy standards, the security standards, and the HHS Office of Inspector General’s Compliance Program for Individual and Small-Group Physician Practices [37], physicians should consider the implementation of a singular, blended program that achieves both meeting the mandatory requirements of HIPAA and also providing the potential benefit from compliance as to issues of fraud and abuse.

**REALITY AND RECOMMENDATIONS**

In conclusion, physicians should recognize that most of the nightmarish scenarios they have heard bantered about are not part of their obligations under HIPAA. In reality, what is most important is that physicians focus on the issues of privacy, electronic transactions, and security; take steps that others on their behalf (business associates and either in-house or outside vendors) are taking measures to comply; that they stand behind and support these measures; and that the practice holds its future focus on actually complying with the new measures. In carrying out these simple steps, physicians not only will be a long way toward compliance with HIPAA but also will find themselves far removed from those who will face the inevitable focus of the federal government.

**REFERENCES**

1. 45 C.F.R. Parts 160, 164.
5. 45 C.F.R. §§ 162.402-162.414.
6. 45 C.F.R. §§ 160.102, 160.103.
8. 45 C.F.R. § 164.534.
23. 45 C.F.R. §§ 160.102, 160.103.
25. 45 C.F.R. Part 162, Subparts I-R.


29. 42 C.F.R. § 424.32(d)(2).


33. 45 C.F.R. § 164.318©.

34. 45 C.F.R. § 164.530(c)(1).

35. 45 C.F.R. §§ 160.103, 164.306(d)(1).

36. 45 C.F.R. § 164.306(d)(3).