Analysis & Perspective

IMPLEMENTING HIPAA

Hospitals, doctors, and other health care professionals—along with employers, insurance companies, and all others who handle individuals' health care information in electronic form—should begin preparing now to meet the high security and privacy standards required by the Health Insurance Portability and Accountability Act of 1996. Compliance requires implementing the technology and operational practices of security systems, which are the framework for enforcing HIPAA's new privacy rules. Initial planning and budgeting for HIPAA projects is best begun now, because statutory compliance deadlines create great time pressure, given the business process reengineering and new systems that are necessary.

Guidelines for Initiating HIPAA Systems Implementing Projects

RICHARD D. MARKS

What's next after Y2K? For the healthcare industry, and for the universe of employers and others who deal with medical records in electronic form, the answer is HIPAA—the Health Insurance Portability and Accountability Act of 1996.[1] HIPAA is an omnibus privacy act for medical records. Regulations to enforce HIPAA will demand significant new security measures from all who handle medical records in electronic form. Unlike Y2K, HIPAA's deadlines are likely to move. HIPAA also will last long past its initial compliance deadlines, affecting healthcare and its costs for years to come.

HIPAA is very real. However, senior managers in the $1.1 trillion healthcare industry[2] are just beginning to develop an initial awareness of HIPAA's complexity and likely impact. By and large, projects to implement HIPAA have not yet started in earnest.

This article offers an introductory briefing on HIPAA's likely requirements for security, which is the handmaiden of privacy. The briefing suggests ways for senior managers at affected hospitals, health plans, and other enterprises to initiate projects for complying with HIPAA's detailed security rules, which probably will become effective before similarly detailed regulations setting forth privacy requirements.

Among other things, managers at healthcare institutions are wary of spending money to deal with government regulations that are not final, and to buy unproven, expensive new hardware and software systems. Yet, once the Department of Health and Human Services (HHS) issues the regulations to implement HIPAA in final form later this year (as now seems likely), most entities will be allowed only two years to comply. This period will be far too short for efficient, cost-effective implementation of the complex new business processes and expensive new software systems that probably will be necessary because of HIPAA. Consequently, senior managers need to begin the planning and budgeting processes now, while conserving money and institutional focus, and avoiding vaporware.[3]

[1] Public Law 104-191, enacted August 21, 1996, codified at 42 U.S.C. § 1320d.

[2] U.S. Department of Health and Human Services, *Health Care Financing Review, Statistical Supplement*, 1999, at 2.

Richard D. Marks is a partner in the Washington, D.C. office of Davis Wright Tremaine LLP, where his practice includes information technology, privacy and security, and health care information systems; he is chair of the Computer Law Division in the ABA's Section of Science and Technology and a director of the Computer Law Association.

[3] The Internet and Technology Desk Reference, by Michael D. Scott, defines "vaporware" as: "Computer software or other computer product announced long before its availability. Usually done to convince users not to purchase a competitor's product."

  ECLR ISSN 1098-5190

Introduction

The part of HIPAA of concern is a federal privacy statute for medical records. Privacy will be protected using new privacy and security standards. As proposed by HHS, these standards are formidable. In order to "ensure" security as required by HIPAA[4] they will require a large proportion of the medical care industry to install new technology for encryption, and to adopt new business processes that are likely to be costly and, in many ways, wrenching.

Because this article is a preliminary discussion of how to meet HIPAA's requirements, and because there are many articles about HIPAA,[5] I start with only a brief outline of the statute and its regulatory scheme. The focus is what to do about HIPAA, and why it is a long path that is best begun immediately.

My conclusion—or current hypothesisis—that the technology required for HIPAA compliance does not exist in systems or packages that can be installed easily or inexpensively, by adding them on to the hardware and software systems now in place at most hospitals, medical centers, and physicians' offices. Instead, the reverse is true. Further, while most major vendors of healthcare software systems are working on appropriate encryption add-on systems for their product lines, these encryption systems are still in development. They are unproven. They also may not indeed, they are unlikely to work with other vendors' systems with which they are interfaced. This presents significant problems to top management at medical institutions throughout the country, where the norm is to have installed a mix of systems from different vendors.

Management also will face substantial challenges in instituting security practices, and all their accompanying polices and other paperwork, that HHS seems intent on demanding under HIPAA. The new security demands—quite apart from the proposed privacy rules—will require true business process reengineering.

Consequently, there is a premium on management's learning about HIPAA in detail without delay, as preparation for the effort to select, acquire, and implement new systems, and adopt new procedures, to satisfy the statute as HHS is interpreting it.[6] For most medical enterprises of any size, the two-year deadline for meeting HIPAA's *security* requirements is likely to be insufficient (even though the starting date for the two-year period for implementing HHS's *privacy* rules probably will be postponed until fall of 2000, because of the huge number of comments about the proposed privacy regulations that were filed with HHS).

Background

The part of HIPAA we are concerned with here is a federal privacy statute enacted to establish and protect patients' privacy rights in their medical records. What is generally referred to as HIPAA is actually the ironically titled "Administrative Simplification" title of a much larger statue amending the Social Security Act, and dealing with, among other things, healthcare insurance portability and Medicare fraud and abuse.

The use of "simplification" in the title reflects Congress's expectation that HIPAA will force the healthcare industry to adopt **electronic data interchange**, or **EDI**, for a range of healthcare administrative and financial tasks, and for many related clinical functions as well. Once the industry makes this transition, Congress hopes, the daily business of healthcare will be much more efficient, because it will be automated. According to Congress, that is likely to save money and improve patient care.

A number of assumptions underlie this approach. Among them is that technology has developed sufficiently so that an industry wide conversion to EDI is feasible within the time, generally two years from the promulgation of HIPAA's final implementing regulations, that Congress set. We will return to this assumption later.

While there is considerable room to argue about whether there is a *widespread* failure of doctors, hospitals, insurers, and others to protect the privacy of medical records,[7] there is little question that the politics of medical record privacy are formidable. There is immense momentum to strengthen privacy protections, a momentum that gains with each month's new revelations of privacy violations on the Internet (though

---

[4] For example, new 42 U.S.C. § 1173(d)(2) states:

SAFEGUARDS—Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—
(A) to *ensure* the. integrity and confidentiality of the information;
(B) to protect against *any reasonably anticipated*—
(i) threats or hazards to the security or integrity of the information; and
(ii) unauthorized uses or disclosures of the information; and
(C) *otherwise to ensure* compliance with this part by the officers and employees of such person.
(Emphasis supplied).

[5] *See, e.g.*, Alexander J. Brittin, Alan C. Brown, and John P. Tedesco, *Understanding HHS's Proposed Health Information Privacy Standard*, BNA's Health Law Reporter, December 9, 1999, at 1949; Nancy L. Perkins, "*What Price Privacy?*" Legal Times, March 13, 2000, at 25.

[6] Security and Electronic Signature Standards; Proposed Rule, 63 Fed. Reg. 43241 (1998) (to be codified at 45 C.F.R. pt.142) (proposed Aug. 12, 1998); Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59918 (1999) (to be codified at 45 C.F.R. pts. 160-164) (proposed Nov. 3, 1999).

[7] *See, e.g.*, California HealthCare Foundation, *Privacy—Report on the Privacy Policies of Practices of Health Web Sites*, January, 2000.

rarely do these celebrated incidents involve medical records).[8] The politics are implacable. What member of Congress can go wrong advocating strong privacy protection for patients' records, or vowing harsh, swift justice to those who would disclose medical records improperly?

The politics of medical record privacy are also turgid. In 1996, in HIPAA, Congress gave itself a deadline of 42 additional months to pass medical record privacy legislation.[9] If Congress missed its own deadline, then the Secretary of Health and Human Services was to propose and adopt appropriate final regulations within six additional months.[10] (That deadline was Feb. 21, 2000, and the Secretary has missed it.) This safety valve is stark recognition of the controversy surrounding all aspects of medical record privacy.

Rulemakings

HHS Secretary Shalala issued a series of proposed rules dealing with privacy and security standards and with the standards for nine common healthcare transactions (such as making a claim for reimbursement from an insurer or other payor), patient and provider identifiers, and digital signatures. While none of these areas lacks complexity, the more technical areas of computer operations, such as transaction standards, are proceeding apace. The same cannot be said of the proposed privacy regulations and, to a lesser but still significant extent, the security regulations.

The implementing regulations define "**protected health information**," or "**PHI**," as individually identifiable health information transmitted or maintained in electronic form (or derived from electronic form, such as a printout from a computer), but not the same information if it is only on paper (and has not been printed from an electronic record)."[11] "**Covered entities**" are hospitals, health plans, health clearinghouses, and others, such as employers, that hold, use, or transmit PHI.[12]

Transaction Standards

The transaction set standards[13] are massive compendiums of computer code notations. They systematically assign labels to the myriad transactions common to the furnishing of, and payment for, medical care. The sets are available free from HHS's HIPAA website."[14] While they are unexciting reading, a short time spent reviewing any one of the transactions sets can give senior managers an appreciation for the subject matter and level of detail that HHS, under HIPAA, seeks to standardize in electronic data interchange for the healthcare industry.

The final transaction set rules are now expected to be released in June 2000, with an implementation deadline of June 2002. They cover: first report of injury, health plan eligibility, healthcare claim attachment, healthcare claim status, referral certification and authorization, premium payments, health plan enrollment and disenrollment, claim payment and remittance advice, and healthcare claim or encounter.

What is this list? It includes the basic transactions associated with an insured patient's participation in a health plan, from entering the plan through receiving reimbursement for care. The amount of paper-based and computer processing presently associated with these transactions is staggering. Administrative costs of the current system may account for more than 20 percent of the total healthcare costs in the U.S.

Standardized computer codes for these transactions are essential for automated process of patients' claims for care, because those claims involve data exchanges among the healthcare, insurance, and financial industries, as well as the federal government. Standard setting is often an appropriate governmental function, particularly when the market has not, or cannot, establish de facto standards. By and large, the development of these healthcare transactions sets, which began during the Bush administration, is neither controversial nor alarming.

Privacy Standards

The same cannot be said of HIPAA's privacy standards. The Secretary's proposed rules take almost 150 pages in the Federal Register, and they generated, according to recent statements from HHS officials, approximately 250,000 comments from 50,000 commentators.

The comments predictably fall into two general categories, arguing either that the rules do not go far enough to protect patients' privacy rights in their medical records or that the privacy regime is overly complex, too difficult to comply with or administer, and too costly.

This is not the place to attempt distillation of the issues exploding from this mass, and for purposes of this analysis we need cover only a few illustrative points. The regulations require a patient's explicit written consent for some purposes, such as a hospital's fundraising or commercial marketing by a

[8] There are of course problems surrounding the privacy of health information on the Internet, such as the downloading by drug companies of prescription data sent to pharmacies by customers who are filling prescriptions, as contrasted to patient data maintained by hospitals or physicians.

[9] Public Law 104-91, Sec. 264(c)(1).

[10] *Id.*

[11] Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. at 59937-38.

[12] *Id.* at 59924.

[13] Health Insurance Reform: Standards for Electronic Transactions, 63 Fed. Reg. 25272 (1998) (to be codified at 45 C.F.R. pt. 142) (proposed May 7, 1998); *see also*, National Standard Health Care Provider Identifier, 63 Fed. Reg. 25320 (1998) (to be codified at 42 C.F.R. pt. 142) (proposed May 7, 1998); Health Insurance Reform: National Standard Employer Identifier, 63 Fred. Reg. 32784 (1998) (to be codified at 45 C.F.R. p. 142) (proposed June 6, 1998).

[14] http://aspe.hhs.gov/admnsimp/

hospital or other business. In contrast, generally a patient's consent is not required for purposes of treatment, payment, or healthcare operations (the precise scope of these terms is at issue). However, the proposed privacy regulations would require custodians of medical records to disclose only the minimum information necessary for a particular clinical purpose. Whether this rule makes sense at all, whether it is precisely the opposite of the correct approach, and who would make this "minimum necessary" judgment—under what circumstances, how, and how quickly—are all disputed in the comments.

The proposed privacy rules also require hospitals, physicians, and other covered entities to use **business partner agreements** to ensure that those with whom they do business, and with whom they exchange PHI, follow the covered entity's privacy policies and meet the covered entity's privacy standards.[15] A covered entity must have business partner agreements with, among others, its lawyers and accountants. One proposed required feature of these agreements is a third party beneficiary clause, giving the patient a private right of action against the covered entity and its business partner if PHI is alleged to have been wrongfully disclosed. Many interested commentators argue that the statute does not give HHS the power to create a private right of action, and HHS's insistence that it can do so is will likely be litigated early in HIPAA's implementation.

Security Standards

So much attention has been paid to HHS's proposed privacy regulations that the proposed security standards have been pushed to the background. However, the security standards, if adopted in anything close to their proposed form, will have an enormous impact that is *independent of the privacy rules*, whenever and in whatever form they are adopted. Further, the security standards are likely to be adopted in fall 2000 (months before HHS issues the final privacy rules), making the compliance deadline sometime in the fall of 2002, which again is *independent of, and probably some months earlier than, the deadline for complying with the final privacy rules.*

Section 262 of HIPAA adds a new set of security requirements for covered entities:

> [to] maintain reasonable and appropriate administrative, technical, and physical safeguards … to *ensure* the integrity and confidentiality of [PHI] … to protect against any reasonably anticipated … threats or hazards to the security or integrity of the information; and … unauthorized uses or disclosures of the information; and … otherwise to *ensure* compliance with this part by the officers and employees of such [covered entity].[16]

The use of "ensure" and "any reasonably anticipated" create a very high standard, both legally and practically. Congress did not elect to require those who handle PHI to use a standard of "prudence" or "reasonableness under the totality of the circumstances," or a comparable word formula. Rather, those who deal with PHI must protect against any threat that a prudent manager can reasonably anticipate, and *ensure*—essentially, guarantee—that the ironclad safeguards contained in the enterprises' written security policies are followed without exception. Failure to meet this high standard invites criminal action and civil penalties under HIPAA, and potentially exposes the institution and the staff members involved to civil liability from private plaintiffs asserting a variety of theories.[17]

How does this very high standard of security relate generally to security developments in government and corporate communications, including the Internet? The prudent business executive's perception of the magnitude of security threats is growing to match industry experience. Information security standards of care under the business judgment rule[18] and state tort and consumer protection law are rising concomitantly. This trend is reinforced by a rapidly growing sophistication in corporate security practices, including the technology now employed for security purposes, particularly as business generally responds to the increasing sophistication of hacker attacks. Meanwhile, government at all levels, and particularly the federal government, is devoting more and better resources to countering high technology crime. All of these trends should be considered in evaluating the "any reasonably anticipated" threat standard in HIPAA. No doubt this is a very high bar, and one that is constantly ratcheting upward.[19]

Reading HHS's proposed security standards reinforces this conclusion. In 49 pages in the Federal Register, HHS lays out a comprehensive security scheme. It includes administrative procedures, physical safeguards, technical

---

[15] Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. at 59948-50.

[16] New 42 U.S.C. 1173 (d) (2) (emphasis supplied); see note 4, above.

[17] *See* the discussion below under "Criminal and Civil Penalties."

[18] *See In re Caremark International Derivative Litigation*, 698 A.2d 959 (Del Ch. 1996) (even though directors and officers may not be liable for wrongdoing that they have no reason to suspect, they have an affirmative duty to establish a compliance system); *see also Kahn v. MSB Bancorp., Inc.*, 24 Del. J. Corp. L. 266, 1998 WL 409355 (Del. Ch.) (protection under the business judgment rule may be lost through gross negligence); *In re Baxter International, Inc. Shareholders Litigation*, 654 A.2d 1268 (Del. Ch. 1995) (permissible under Delaware Code for corporation to exempt directors from personal liability, and plaintiff must then show bad faith, intentional misconduct, or knowing violation of law); *Smith v. VanGorkom*, 488 A.2d 858 (Del. 1985) (board decision must be "informed"); *Graham v. Allis-Chalmers Mfg. Co.*, 188 A.2d 1269 (Del. 1963) (directors have no duty affirmatively to seek out corporate employees' wrongdoing).

[19] *See generally The T.J. Hooper v. Northern Barge Corporation*, 60 F.2d 737 (2d Cir. 1932) (standard of care is raised by the availability of technological innovations).

security services, and technical security mechanisms, and requires covered entities to address all aspects of security in a concerted fashion.

Among the areas for which a covered entity must develop written policies and institute business processes are: physical security (physical access control, secure workstations, and security policies for work station use), personnel security, procedural security (formal mechanisms for processing records, information access control, internal audits, security management processes, termination procedures for departing employees and others), security incident procedures to "ensure" prompt reporting and handling of security violations, security awareness training, and contingency plans.

"Security configuration management" is necessary so that hardware and software changes do not create new security weaknesses. Technical security services and technical security mechanisms include access controls, data and entity authentication, authorization controls, and audit trails, plus integrity controls, abnormal condition alarms, event reporting for operational irregularities, and *irrefutable* entity authentication.

Take as an example the requirement to create secure workstations, and control the access to them. The proposed privacy regulations state:

> Each organization would be required to put in place physical safeguards to eliminate or minimize the possibility of unauthorized access to information. This would be important especially in public buildings, provider locations, and in areas where there is heavy pedestrian traffic.[20]

This requirement should be read in the context of other parts of the proposed regulations assigning security responsibilities to specific individuals (all doctors, nurses, and office staff with access to PHI included), placing controls on storage media, mandating physical and technological access controls, requiring written polices on workstation use and on authorization to assure use of PHI only by properly authorized individuals, and requiring audit controls. This is not an exhaustive list.

Imagine how a hospital would implement these requirements in practice. How can all these rules be followed in a cost-effective way, without impairing patient care? Is it feasible to make each nurses' station in a hospital a secure area, from which patients, patients' families, and others are separated by effective physical barriers? How much would that cost? How inconvenient would that be for all involved?

How will each doctor and nurse log into the system to check patient records? Each look must be logged and an audit trail established. This means getting in and then logging out quickly and securely. Some form of biometric identification (*e.g.*, a thumbprint scan), in combination with a smart identity card, may be needed to satisfy requirements for certainty, speed, and convenience. Who can point to a hospital where this sort of setup exists now? Does it seem a good way – efficient for staffs and patient and family-friendly — to configure a hospital?

HHS's proposed security standards also require use of "**chain of trust partner agreements**" with all entities (or people) who are in the chain down which a covered entity transmits PHI.[21] While chain of trust partner agreements at first seem duplicative of the business partner agreements required by HHS's proposed privacy standards, they are somewhat different and are, in any event, a requirement as things now stand. (We do not know whether HHS will insist that the model chain of trust partner agreement include a third party beneficiary clause that creates a private right of action. Doing so would raise the same controversy as under the privacy standards whether HHS has any power to create a private right to sue that is not in the statute itself.)

Implementing a comprehensive security program with these features will require extensive business process reengineering, even at major medical centers that already have what has been considered, up to now, to be a high level of security. In other words, facilities are ahead of the game if they have closed-circuit television monitoring; badges, cipher locks, and other physical access controls; security specialists in the information systems department; firewalls, automated anomaly or intrusion detection systems, and comprehensive access and use logging systems. Conversely, smaller or less sophisticated hospitals have a greater distance to travel.

However, even the most sophisticated medical centers are unlikely to come close to meeting HIPAA's security standards. In effect, and whether unintentionally or not, HIPAA requires the healthcare industry to begin treating medical records in the same way that the federal government treats national defense secrets — as a form of classified information. Whether that is wise policy is for another time. What is vital now is that senior management realize the impact of the new security requirements and begin planning, and budgeting, for them.

Further, everyone in the healthcare industry should realize that HIPAA's security requirements will usher in a regime of personnel security,[22] and surveillance of healthcare professionals and their colleagues, that generally is familiar only within the defense establishment. Why? Because personnel security and surveillance are necessary elements for a comprehensive security plan. Without them, the other elements are too easily evaded.

Most of the practical and policy implications of these

[20] Security and Electronic Security Standards; Proposed Rule, 63 Fed. Reg at 43253.

[21] *Id.* at 43252.22.

[22] Id. at 43252, 23266.

facts of life are also for another time, not for an introductory essay. Note, however, that effective personnel security, whose modern practice was pioneered, and the standards set, by the defense and national security establishment, is enormously expensive and delay ridden.[23] Aside from the operational inconvenience and inconvenience of adhering to everyday operational procedures such as access and authentication controls, good personnel security requires initial and recurring background checks of all who come in contact with protected information (PHI in HIPAA's case). Realize too that health professionals and their staffs are likely to express an intense dislike of having systematic surveillance techniques used against them, creating constant coverage of both their use of healthcare computer networks and their physical comings and goings at hospitals, clinics, and offices.

The Encryption Layer

Although HHS's proposed security standards do not require use of encryption except over open networks,[24] the practical reality is that *covered entities will have to implement encryption both internally and for external communications involving PHI in order to meet HIPAA's statutory standard, as well as any likely final security rules that HHS adopts*. The encryption technology will be some form of asymmetric encryption, that is, some form of **public key infrastructure** or "**PKI**" (PKI typically includes the capability to generate and use digital signatures.)

My working hypothesis is that there is no encryption system product currently available that will, as a practical working matter, enable covered entities to encrypt their patient registration and scheduling systems, clinical systems (order entry, radiology, laboratory, and so forth), and billing and administrative systems in a way that is sufficiently fast or free from errors, and that will meet HIPAA's security standards. It is true that the major vendors of healthcare information systems are working furiously to develop encryption add-ons for their own particular information systems, both already installed and in development. Even those add-ons have yet to be proven in actual use.

However, even the major vendors' hardware and software systems in hospitals and medical centers today are not end-to-end systems. Rather, these systems usually are interfaced, sometimes well and sometimes inelegantly, with systems supplied by other manufacturers. They deal with patient registration and scheduling, hospital and physician services, laboratory results, radiology results, billing, and myriad other details. All these elements are necessary for clinical services, administrative functions, and to enable payment. I know of no healthcare facility where encryption meeting HIPAA's proposed security standards (or any comparable comprehensive standards) has been successfully implemented. Those who work on systems projects from a technology, business, or legal perspective well know how important it is for systems such as this to be proved in practice. Similarly, experienced systems managers know that the development and tailoring of new systems to meet the demands of actual business operations can take far longer, and cost more, than early estimates.

For that reason, a model such as PCASSO[25] is useful, but (to my knowledge) has not been interfaced with patient registration and hospital and physician billing systems, end-to-end in an integrated hospital computing system environment, in any actual operations. Doing so would not be an easy, quick task, with a predictable budget. As the engineers say, it would be "nontrivial."

Putting an encryption system into a hospital or medical center so that it works end-to-end, internally and with external entities such as clearinghouses and payors, would be a very substantial task, even with proven systems. Until a vendor can point to effective working interfaces of a sophisticated encryption system with the variety of legacy systems used in hospitals today, and demonstrate their efficient, integrated operation and the ability to handle the substantial transaction volumes that occur day-to-day, senior executives should be very skeptical of statements that appropriate encryption technology is mature and available. After all, how many hospitals use encryption on their e-mail systems? And e-mail is commonplace and relatively simple compared to patient

[23] *See* Walter Pincus, *900,000 People Awaiting Pentagon Security Clearances*, The Washington Post, April 22, 2000, atA7 (describing the "huge backlog" of unprocessed clearances, the background investigations necessary to justify granting clearances, and the computer problems plaguing the Defense Security Service, the agency responsible for Department of Defense security clearances; the article reports that a $100 million computer system installed to handle the clearances was inadequate, and required an additional $47 million investment).

[24] Security and Electronic Security Standards; Proposed Rule, 63 Fed. Reg at 43256.

[25] The PCASSO (Patient Centered Access to Secure Systems Online) Project is a joint effort of Science Applications International Corporation (SAIL) and the University of California, San Diego (UCSD), operating under a grant from the National Library of Medicine (NLM) from October 1996 through September 1999. It is operated at UCSD, has almost 300 active users and contains the medical records of 178,000 patients. It includes interfaces to laboratory and medications ordering systems, but does not appear to have been interfaced with hospital or physician billing systems, patient scheduling systems, and the like, all of which are essential to hospital operations and will in all likelihood be covered by HIPAA's security and privacy requirements. Further, it was not designed to cover other vital systems such .as electronic mail. PCASSO has a wide array of security features designed for use when connected to the Internet. "The purpose of the experiment was to determine whether state of the art security technology and assurance methods ... would enable [healthcare] consumers and their providers to access highly sensitive patient information on the Internet safely and effectively." Dixie B. Baker, "PCASSO: A Model for Safe Use of the Internet in Healthcare," Journal of the AHIMA, March 2000, at 33, 34.

scheduling and clinical software, and hospital and physician billing systems (and particularly to end-to-end, integrated versions of these systems, which some vendors plan to offer). Experience to date is that commercially available encryption systems are slow in operation and require substantial effort before they can be rolled out to the public.[26]

Criminal and Civil Penalties

These concerns take on an urgency because of HIPAA's criminal penalties. Wrongful disclosure of individually identifiable health information carries up to a year in prison and up to a $50,000 penalty. If the wrongful disclosure is under false pretenses, the maximum term rises to five years, and the monetary penalty to $100,000; add an intent to sell, transfer, or use for commercial advantage, personal gain, or to inflict malicious harm, and the prison term increases to a maximum of 10 years, with a monetary penalty of up to $250,000.[27]

It is unlikely that most doctors, nurses, hospital administrators, or information system staff members (to name a few) ever expected to be exposed to these levels of jeopardy.

HIPAA also has civil penalties of $100 for violation of a single provision, with an annual cap per entity of $25,000 for violations of an identical requirement or prohibition.[28] Failure to implement the transaction sets is $25,000 annually per set, for an annual maximum for all nine sets of $225,000.[29]

Covered entities that fail to comply with HIPAA's privacy and security standards also must consider potential liability in tort, including invasion of privacy (publication of private facts, false light, and unauthorized commercial use, as the case may be), defamation, and fraud. There is also potential exposure under consumer fraud statutes. And, of course, there are various potential causes of action for breach of contract, depending on the circumstances.

Public companies in the healthcare industry face additional exposure from shareholder suits if they fail to implement adequate information security programs.

HIPAA and Electronic Commerce

HIPAA will force the healthcare industry to move into electronic data interchange much more rapidly than would otherwise be the case. Indeed, Congress sought to achieve the efficiencies of EDI in healthcare by enacting HIPAA. Therefore, while complying with HIPAA is a substantial management challenge, and probably a major (and, for many institutions, an unexpectedly large) expense, it will also be a catalyst for hospitals and academic medical centers, as well as physician practices, to develop e-commerce strategies.

Legislative Approaches

Achieving HHS's contemplated level of privacy of medical records will require a concomitantly high system of security, which means that healthcare professionals will be accorded little or no privacy as they go about their daily tasks. Privacy begets security.

HHS's proposed privacy and security standards will impose burdens are so substantial that new efforts to convince Congress to amend HIPAA are inevitable. Little is likely to happen in this election year. In 2001, however, expect an intense political debate about the nature and extent of security regulation needed to achieve an adequate, cost-effective, sensible level of privacy for medical records.

Checklist for HIPAA Compliance Projects

The scope and breadth of HHS's proposed security and privacy regulations are daunting. Taken together, these regulations envision physical settings, electronic infrastructures, and day-to-day routines for ministering to patients that, in many important respects, are very different from the way patients receive care today, and less appealing. Nevertheless, expecting a substantial alteration of the implementing regulations from HHS seems unrealistic, at least at this juncture.

Moreover, the clock is ticking. Few healthcare institutions have the capability to become expert about systems that can be used to satisfy HIPAA's privacy and security rules, and then acquire and implement them in two or two-and-a-half years. There simply is too much to do, even if mature (well-known, tested) technology to satisfy HIPAA were available in the marketplace, which it is not. If HIPAA's present compliance deadlines hold, there will be a crunch toward the end of 2002.

Here are suggestions for initiating HIPAA projects, keeping in mind the objectives of avoiding new, untested encryption and other systems, conserving money, and maintaining institutional focus:

- Arrange for briefings about HIPAA's legal requirements. The briefings should cover the transaction set standards and the proposed security and privacy rules, all in the context of what the statute itself demands. Concentrate on the legal standards of care that will apply to various aspects of the enterprise's operations. Some of this analysis can be done in memoranda, while other parts are best done face-to-face. The legal standards of care are a foundation for assessing how much must be done to satisfy HIPAA.

- The security standards will come first in time, and the privacy rules will, metaphorically, plug into the security infrastructure. Look first to the security requirements.

- The proposed rules require each covered entity to

[26] *See* Julia Angwin, *Internet Encryption's Password is "Slow,"* The Wall Street Journal, March 28, 2000, at B8.
[27] Public Law 104191, Sec. 262, codified at 42 U.S.C. Sec. 1177(b).
[28] Public Law 104-191, Sec. 262, codified at 42 U.S.C. Sec. 1177(b).
[29] *Id.*

perform a *security evaluation*.[30] This means finding a consultant that can perform a *penetration analysis* of an enterprise's current computer and telecommunications networks, and advise about security vulnerabilities and how to counter them. Few healthcare organizations have ever had this kind of an analysis performed. The experts hired to do the work should consult beforehand with attorneys who are knowledgeable about HIPAA's security requirements, so that the review will be adequate to meet the requisite standard of care. Note that the proposed rule also requires "certification" of computer networks by internal or external means.[31] The standards to be used for this certification are undeveloped, and the path to their development is unclear. At the least, maintaining certification will require recurrent vulnerability analyses and upgrades to incorporate improved technology for countering known threats.

- With HIPAA's standard of care as a constant reference, formulate a plan for learning about encryption and other security products that may be available, now or in the next 12 to 18 months, for installation in your enterprise. This will probably at the least involve use of requests for information (RFIs). The new systems will need to be compatible with the institution's existing, or "legacy," systems. If legacy systems cannot be protected using encryption, as will be true in some cases, the legacy systems probably will have to be replaced by the deadline (sometime in fall 2002). For a hospital, for example, this means protecting patient registration and scheduling, clinical, and hospital and physician billing systems, along with most email systems and, probably, some other management systems. This typically will involve consultation with the several vendors of the existing systems, and with systems integrators who may be called in to help with the installation.

- Evaluate the enterprise's strategy for electronic commerce. This strategy should be melded with the strategic approach to complying with HIPAA.

- Review the costs and risks associated with a systems implementation project, or projects, of this scope. (The risks arise because large computer or software installation projects often are late, over-budget, and result in systems that under-perform. This is generally as true of healthcare as other fields.) There will be a substantial set of related budgeting, operational, regulatory, and contractual issues. The greatest risk will entail assessing the feasibility of installing untried systems, or untried combinations of systems. Some, but not all, of this risk can be mitigated contractually. In any event, the initial round of planning and budgeting will be more useful if it includes a sophisticated evaluation of these risks and their associated costs.

- Evaluate all future purchases of systems or clinical equipment in light of HIPAA's proposed rules. Will monitors have sufficient security features so that only authorized personnel have access to the data (which are likely to be PHI) they generate or display? Can new software systems be encrypted at reasonable cost, and without degrading performance? Will they communicate efficiently with other encrypted systems, both internal and external? Will new buildings, or renovation projects, have to be redesigned to incorporate physical access controls to secure areas?

- Prepare an initial draft of the various *policies* required under the proposed *security* regulations (which, due to the stringent requirements in the statute, are unlikely to vary in their ultimate requirements), and *skeleton* policies under the *privacy* regulations. This will furnish an initial look at what the enterprise will face in changing its physical plant and operating procedures to meet HIPAA. For example, a hospital may conclude that it must redesign all its nurse's stations to assure that only authorized individuals can have access to them. It may need to install smart-card and biometric access controls. It will need to designate security officers, and may have to hire additional security staff. It probably will have to institute new personnel screening procedures for new and existing employees. *Further, all these policies will be at issue when complaints are filed alleging violations of patients' medical record privacy rights. Consequently, the policies are legal documents as much as they are operating guidelines.* They will be front-and-center in litigation. At the same time, they must be designed to reduce operating burdens as much as possible under the circumstances.

- Approach with a high degree of skepticism claims that affordable, tested encryption systems are available now in the marketplace. Most senior managers are well aware of how much effort is necessary to make existing systems function well today. Imagine the engineering task of installing a layer of encryption technology, all of which carries overhead on the system, so that all the enterprise systems can continue to communicate with each other *and with external systems (such as those of payors)*, allow fast response and sufficient throughput, *and safeguard all the systems from attacks or unauthorized use from without and within.*

An early start on planning and acquiring information about security technology and operating procedures, and the legal standards they must satisfy, will pay dividends throughout the next two to three years.

[30] Security and Electronic Security Standards; Proposed Rule, 63 Red. Reg. at 43251.
[31] *Id*.