SCOTTSDALE INSTITUTE

INFORMATION EDGE

A CEO Resource for Managing Clinical Information Systems

October 1999
Volume 5, Number 8

HIPAA Comes Home

The latest word on federal rules for healthcare information

Guest Editor: Keith MacDonald, First Consulting Group

Executive Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) will impact all healthcare organizations over the next two years similar in magnitude to the effects of Y2K. For many, the electronic commerce components of HIPAA represent not just changes in technology but in a whole new way of conducting business. Many would—and should—think about HIPAA as an opportunity to reduce administrative overhead and streamline work processes. HIPAA is really a smart business move—penalties or not.

Along with standards for electronic transactions, HIPAA spells out specific measures that all organizations must implement to protect patient privacy. Contrary to general practice, technical measures alone will not spell compliance. Finalized rules for the electronic transaction standards and security are on track for final publication by the end of 1999 and will look largely identical to the proposed rules released last year. Organizations will have roughly two years to achieve compliance. Knowing the complexity of the processes associated with electronic transactions and the effort required in undertaking the implementation of an effective organization-wide security program, two years will barely be enough time.

After getting senior leaders educated on the impacts of HIPAA, organizations should begin by assessing current practices against the known HIPAA standards. Complying with security standards can be a daunting and elusive task. Security must start at the leadership level of the organization and must be perpetuated with a *confidentiality-conscious culture.*

In the main text of this Information Edge, Keith MacDonald of First Consulting group provides a step-by-step process for complying with HIPAA regulations.

▲

SCOTTSDALE INSTITUTE
MEMBERSHIP SERVICES OFFICE
1660 SOUTH HIGHWAY 100
SUITE 140
MINNEAPOLIS, MN 55416
(612) 545-5880
FAX (612) 545-6116
EMAIL scottsdale@fcgnet.com

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) will impact all healthcare organizations over the next two years. Do you know if your organization is ready? New standards for electronic transaction processing will touch many information systems and most key business processes within both health-delivery and health-plan segments of healthcare. Increased levels of security and protections for privacy and confidentiality will change the way *all* organizations deploy technology and set policies for maintaining the security and privacy of patient information. The impact may be similar in magnitude to the effects of Y2K and implementation must be completed within the next two years. Where did HIPAA come from and why is it such a big deal? Let's review the origin and components of HIPAA to better understand its impact.

For more information, contact Keith MacDonald in First Consulting Group's Boston office at 781-402-2520.

Keith MacDonald
First Consulting Group

For many the electronic commerce components of HIPAA represent not just changes in technology but a whole new way of conducting business.

Healthcare has been struggling for many years with a lack of standards, sadly paying the price in higher administrative costs. The banking industry long ago adopted standards that support international commerce—witness the ubiquitous ATM machine—but healthcare has been unable to move to similar consensus. While many healthcare standards exist, they too often apply to a discrete process or technology component. In 1996, the industry finally banded together with support from Congress and succeeded in including electronic transaction standards in a piece of marginally-related legislation now known as HIPAA. These standards were not newly created; in fact, HIPAA mandates the endorsement of de facto standards where reasonable ones already exist. In the case of certain electronic transactions, those standards do exist. (See sidebar)

Electronic Transaction Standards
HIPAA mandates compliance with certain standards for the following transactions when conducted electronically:

- Claims
- Payment and remittance
- Coordination of benefits
- Claim status
- Enrollment and disenrollment
- Eligibility
- Premium payment
- Certification and authorization

The clinical codes used in each transaction must also be standardized on ICD-9, CPT-4, CDT, HCPCS and NDC.

What's the Big Deal?

So, why would HIPAA be such a big deal, then, if the standards are already widely known? Certainly the associated penalties will motivate some organizations to comply if they don't already. For some organizations that conduct these electronic transactions even today, complying may not be so large a task. For many, however, the electronic commerce components of HIPAA represent not just changes in technology but a whole new way of conducting *business*. Many would—and should—think about HIPAA as an opportunity to reduce administrative overhead and streamline work processes. Electronic commerce can do just that by reducing paperwork, labor-intensive data entry and rework. Though some organizations are rumored to be ready to accept the consequences and pay the penalties rather than conform, compliance with HIPAA is really a smart business move—penalties or not.

Healthcare security is lacking

Hand-in-hand with healthcare's lack of transaction standards are its often lax security practices. A 1997 Institute of Medicine study found that sound measures for protecting confidential patient information are gen-

erally lacking across the healthcare industry. Breaches of patient privacy—and the accompanying outcries of patient privacy advocates—can be seen regularly in our mainstream press. The security components of HIPAA are intended to address this issue. Along with standards for electronic transactions, HIPAA spells out specific measures that *all* organizations must implement to protect patient privacy. Contrary to general practice, technical measures alone will not spell compliance. (See sidebar)

Why are some organizations not moving forward?

According to the 1999 HIMSS Leadership Survey, less than a fifth of provider organizations surveyed had begun implementing their HIPAA-related security programs. Electronic data interchange (EDI) migration is moving equally slowly. CIO's and others cite two concerns: a lack of IT resources due to the current focus on Y2K, and a belief that, if the standards aren't yet finalized, why start now (and aren't they likely to change or go away anyway)? The truth is that HIPAA is coming. The Dept. of Health and Human Services is legally mandated to execute HIPAA and only an act of Congress could repeal that forward motion. Sadly, some less-than-astute observers have mistakenly interpreted the current debate about the national patient identifier and patient privacy and its associated delays as indicative of a postponement of the whole of HIPAA. This is not the case. In fact, the finalized rules for the electronic transaction standards and security are on track for final publication by the end of 1999 and will look largely identical to the proposed rules released last year. Forward movement is hardly uncertain at this point.

Security Standards
There are 34 specific security requirements under HIPAA, organized into four categories. Some examples include:

- *Administrative:* incident procedures, termination procedures, user training
- *Physical:* media controls, physical access controls
- *Technical:* audit control mechanisms, data authentication, user authentication
- *Network:* alarms, message authentication, event reporting

Specific technologies are not stated or required under HIPAA; organizations must determine appropriate security technologies for deployment based on their own risks and needs.

Compliance with HIPAA is really a smart business move—penalties or not.

Less than a fifth of provider organizations surveyed had begun implementing their HIPAA-related security programs.

The Clock Starts Ticking

Once the final rules are released, the clock starts ticking. Organizations will have roughly two years from this date in order to achieve compliance. And knowing the complexity of the processes associated with electronic transactions and the effort required in undertaking the implementation of an effective organization-wide security program, two years will barely be enough time.

Where Do Organizations Begin?

After getting senior leaders educated on the impacts of HIPAA, organizations should begin by assessing current practices against the known HIPAA standards—for both EDI and security. To some extent, complying with the transaction standards is more straightforward. Though re-tooling manual workflow for electronic processing can be complicated, the electronic standards are clearly specified and not left to misinterpretation. The organization's current or planned breadth of deployment of elec-

tronic transaction processing becomes a consideration, but once the decision is made to move to electronic processing, work can begin.

A methodical EDI approach includes several steps that involve answering a series of questions:

- *Strategic Planning*—What are our organization's key business goals? Can EDI become a key enabler?
- *Assessment*—If we are to proceed with EDI, what are our current capabilities? Do our systems employ the ANSI-standard transaction formats? Do our HIPAA-governed transactions employ the soon-to-be-approved standard code sets? Can we replace current identifiers with the HIPAA standards once they are finalized?
- *Implementation Planning*—What will it take for us to convert our current work to comply with the HIPAA standards? Which work processes must change? Which systems must be upgraded? What about our trading partners—are they ready? What will our project plan look like (time and resources)? What will be our measures of success?
- *Implementation*—How do we execute our plan?
- *Assessment and Monitoring*—Are our processes working as we had expected? Are adjustments necessary?

Some observers have mistakenly interpreted the current debate about the national patient identifier and patient privacy and its associated delays as indicative of a postponement of the whole of HIPAA. This is not the case.

Much like any system implementation, EDI transformation begins with a look at key business processes and is successfully executed with strong project planning.

Security risks

Complying with security standards, on the other hand, can be a more daunting and elusive task. With no specific technology requirements stated in the proposed rules (and none expected in the final ones) organizations must determine the appropriate technologies for deployment based on their own risks and needs. Security risks originate either internally or externally and both must be addressed. Though cyber breaches are highly publicized, internal breaches represent a more common threat. Lax policies that fail to uncover and punish employees who pull up colleagues' personal health information on the computer represent a bigger risk for many organizations.

A real-life example: the daughter of a hospital employee used her mother's password to look up medical records and then called patients with false positive HIV results. A near tragedy—and further negative publicity for the hospital—occurred when one of the patients called attempted suicide[1]. This incident and others like it reinforce the need for sound organizational security policies.

Technology alone is not enough

HIPAA reinforces what organizations with successful security practices have known for years: technology alone is an insufficient solution. Sound security programs include organizational, process and technology components. Security must start at the leadership level of the organization and

must be perpetuated with a *confidentiality-conscious culture.* Such a culture dictates that security is everyone's responsibility (not delegated to IT) and ensures that it is never acceptable to misuse or breach confidential patient information. Full leadership support is essential in obtaining buy-in from all corners of the organization. Physicians cannot be allowed special exceptions for password use or be exempt from punishment.

Initially, convincing leadership of their need for involvement in such a demanding healthcare environment is a challenge, but once they're on board, work can begin. Instilling this *confidentiality-conscious culture* can also become more effective through the support of a Confidentiality Steering Committee. Assigning key organizational staff to this committee will ensure broad and balanced participation. Make this a priority. There's nothing like a security breach or a call-to-compliance to motivate the group's efforts. Members should represent Administration, Legal, Human Resources, Information Technology, Internal Audit, Medical Management, Medical Records, Nursing and Risk Management. This team sets the overall tone of the effort and monitors the organization's progress.
Next steps then become more straightforward:

- *Appoint day-to-day responsibility*—Typically a Chief Security Officer, this person should report to a top business—not a technology—executive
- *Determine risks*—An organization's key business goals should determine which processes are most vulnerable and thus represent the biggest risk; security resources must be correlated with risk lest they be wasted
- *Assessment*—How do our current security practices and technologies compare with community standards? What do we need to reinforce? What technologies can we deploy to effectively manage our risk? (HIPAA offers a framework for ensuring basic security requirements are met)
- *Implementation planning*—Ensuring buy-in and effectively deploying good security practices across the entire healthcare organization can become quite challenging
- *Implementation*
- *Assessment and monitoring*—Security is not a one-time improvement effort and must include ongoing assessment and reinforcement in order to maintain effectiveness

While a naïve security officer could simply proceed down the checklist of HIPAA security requirements—or implement all the latest anti-hacker technologies—a security program that lacks organizational context and support will fail.

Though cyber breaches are highly publicized, internal breaches represent a more common threat. Lax policies that fail to uncover and punish employees who pull up colleagues' personal health information on the computer represent a bigger risk.

Where Else Can I Turn for Help?

Several sources exist for obtaining additional information on HIPAA:

- American Health Information Management Association: Http://www.ahima.org/
- Computer-based Patient Record Institute: Http://www.cpri.org/

- Department of Health and Human Services web site: Http://aspe.hhs.gov/admnsimp
- For the Record: Protecting Electronic Health Information: Http://www.nap.edu/
- OPUS Communications/Greeley Education Company (training materials): 1-800-650-6787
- HIPAA transaction implementation guides: Http://www.wpc-edi.com/HIPAA/index.html

Security must start at the leadership level of the organization and must be perpetuated with a confidentiality-conscious culture.

Vendors, consultants and security professionals also offer many approaches for assessing risk and monitoring security effectiveness.

Conclusions and recommendations

An organization's next steps and considerations should include the following:

- Designate a HIPAA coordinator in your organization
- Develop estimates for dollar and staff resources for a HIPAA compliance program
- There's no time like the present to become educated, tackle HIPAA, and in the process, greatly streamline and secure how healthcare organizations conduct their business. And remember: don't just think of HIPAA as a compliance burden; it's actually *a good thing!*
- While many people view HIPAA as an administrative burden, there are clear strategic advantages in adopting HIPAA standards, especially for e-commerce or e-health purposes. Indeed, the original law was intended to streamline work processes and reduce costs. We will cover the process-improvement and economic justification aspects of HIPAA compliance in future issues.
- For a detailed–and still relevant–review of the HIPAA standards and compliance dates, see the July 1998 Information Edge report "HIPAA Update: Administrative Simplification is a Complicated Job."

[1] Robert Davis, "Online Medical Records Raise Privacy Fears," USA Today, March 22, 1995