SCOTTSDALE INSTITUTE

INFORMATION EDGE

Improving Healthcare Performance Through Information Management

January 2001
Volume 7, Number 1

HIPAA Makes Collaborators of Us All

Executive Summary

If there's one thing healthcare providers have been discovering in the early stages of complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it's that they can't do it alone. By its very nature, HIPAA compliance implies collaborating with trading partners and others in the care continuum with whom information is shared.

While there is a difference between the need to create trading partner collaboration and collaboration among competitors, HIPAA seems to be fostering both. These collaborations provide value in the form of transactions among providers and health plans that are faster, cheaper and more consistent than an organization could achieve on its own.

Fortunately, healthcare delivery systems interested in joining forces with others have plenty of options, including several HIPAA-focused collaboratives.

Under the aegis of the Workgroup for Electronic Data Interchange (WEDI), a national effort dubbed "SNIP," for Strategic National Implementation Process, has identified state and regional organizations that are launching HIPAA collaboratives.

SNIP acts as an information clearinghouse for state and regional HIPAA collaborations.

"SNIP's motto is to think nationally but act locally," says Walter Suarez, who chairs SNIP's Regional Efforts Group. "HIPAA will be implemented locally. But we had to coordinate on a national level the rollout, planning, testing and implementation in the next two years of HIPAA regulations," he says.

In this report we examine some of those local and regional efforts and discuss the prospects for success of HIPAA collaboration. We also talk to some healthcare providers about how far they've progressed on HIPAA compliance, and the merits of joining a collaborative. Partners Healthcare in Boston, in particular, represents the type of organization that others can benefit from in a collaborative. One thing seems clear: The most progressive organizations are linking HIPAA compliance with e-health—and both come with strings attached outside the walls of the organization.

▲

SCOTTSDALE INSTITUTE
MEMBERSHIP SERVICES OFFICE
1660 SOUTH HIGHWAY 100
SUITE 140
MINNEAPOLIS, MN 55416
(952) 545-5880
FAX (952) 545-6116
EMAIL scottsdale@fcg.com

Hanging with NEHEN

Among the largest HIPAA-driven collaboratives is the New England Healthcare EDI Network (NEHEN). Ten healthcare organizations, working with Computer Sciences Corporation (CSC), have developed an electronic payment network linking them to payers. NEHEN's secure electronic commerce network handles more than 2.5 million eligibility requests and responses annually using real-time EDI that complies with HIPAA standards.

NEHEN members believe that providing EDI capabilities to their trading partners does not give them a competitive advantage, but rather an opportunity to improve administrative processes for the healthcare community.

In addition to meeting HIPAA regulations, NEHEN also speeds information exchange among members, reduces administrative costs and improves accuracy of eligibility and other processes, leading to reduced bad debts. The main success factor for NEHEN has been getting health plans and providers to work together. Collaboration has enabled members to leverage experience gained by other participants and jump-start the process of HIPAA-mandated administrative simplification.

NEHEN members believe that providing EDI capabilities to their trading partners does not give them a competitive advantage but rather an opportunity to improve administrative processes for the healthcare community. As a result, all intellectual property created for NEHEN is shared among the members. If a member develops a solution that might benefit the group then that solution is donated to NEHEN. Coordinated development and implementation cycles have dramatically shortened the time members would have otherwise needed to reach significant transaction volumes.

NEHEN provides a method to exchange transactions without mandating how the service is delivered to the end user, minimizing the impact of the NEHEN infrastructure and implementation on each member's organization. The only requirement is that all transactions moving across the network must be HIPAA-compliant. Most member provider organizations generate HIPAA-compliant transactions directly from their own management systems. Others use NEHENLite, NEHEN's Web-based application.

No central database

NEHEN delivers a HIPAA-compliant transaction to members' doorsteps. How that transaction is processed within the organization is their choice. Each provider organization has a direct frame-relay connection to each payer, so there is no central database and no central server that NEHEN must maintain.

According to Suarez, regional e-commerce initiatives like NEHEN or the Minnesota Center for Healthcare Electronic Commerce (MCHEC), which the Minnesota Health Data Institute launched in 1994, need to focus on three things. To successfully link health plans, providers, employers, state government and other regulatory agencies, they need to coordinate HIPAA implementation through educational seminars, reviews and evaluations of proposed and final regulations, and convening of working groups to develop standards. They should provide a telecommunications network to link all parties. Finally, they should conduct e-health projects to meet community-driven needs in such areas as data security.

Boston-based Partners Healthcare is reaping the fruits of having tackled issues like privacy and confidentiality before they were mandated by HIPAA. "Now, we have a launching pad," says Karen Grant, corporate direc-

tor of health information services for the five-hospital integrated delivery system, which includes Massachusetts General and Brigham and Women's hospitals.

While Partners is a leader in addressing HIPAA compliance issues, Grant is quick to point out that the organization has not acted in a vacuum. Collaboration on information standards in the original WEDI group set her on the path to being proactive in the area, she says, and that was followed up with participation in HIPAA conferences, the Scottsdale Institute HIPAA roundtables and NEHEN. Grant and her team also profited from seminars on security and other issues sponsored by the Massachusetts Health Data Consortium.

For more information on HIPAA collaboratives, HIPAA in general or to get involved in WEDI SNIP, visit their Web site at www.wedi.org and click on the "SNIP" button. Information on the New England Healthcare EDI Network is available at www.nehen.org.

Everyday HIPAA

Three years ago, Partners CIO John Glaser asked Grant to gather a task force of health-information directors from the system's hospitals to make sure everybody within the organization was aligned in terms of privacy and confidentiality policies. The outgrowth of those early meetings included a brochure for patients describing the organization's confidentiality policies—now a requirement of the recently released HIPAA privacy regulations.

Partners also developed a medical information release form that must be signed by each patient before their records can be shared. Grant was pleased to have that piece also mandated by HIPAA because it made adoption of the release form easier. Other projects: confidentiality agreements vendors must sign "before they come in the door;" and confidentiality agreements employees must sign at each yearly evaluation.

"The key is to integrate policies and procedures into regular processes."

"The key is to integrate HIPAA policies and procedures into regular processes," says Grant. A Partners hardware security task force decided on a strategy of clustering functional areas—research, clinical and so on—behind separate firewalls instead of having one huge firewall for the entire organization. "Account management" was automated to ensure that a terminated or transferred employee's access to electronic records was appropriately modified or curtailed. E-mail guidelines for employees and affiliated physicians were published. The security team is currently evaluating use of laptop computers and palm devices to develop guidelines for their use, including at home.

Partners automated "account management" to ensure that a terminated or transferred employee's access to electronic records was appropriately modified or curtailed.

Partners used an outside consultant to help conduct a security-risk analysis that involved identifying top areas of concern for departments, resulting in 10 initial security projects, including disaster recovery and business-process engineering. A similar analysis for privacy netted 12 projects, including awareness and training, documentation and naming a privacy official. Again, because of Partners' relative experience in addressing the issue, management is likely to fill the latter position from within the organization rather than having to hire someone from outside.

Would have done it anyway

In response to HIPAA transaction code sets, Partners came up with eight transaction projects, including system assessment, benefits analysis and business-project redesign. Six code-set projects were also identified, including system assessment and remediation plan.

Grant offers what is perhaps her biggest lesson learned: most of Partners' HIPAA-compliance efforts are in one way or another initiatives that the organization would have done anyway as part of developing into an e-health player. Indeed, most of the cost of HIPAA will arise from operational costs like tracking implementation of projects as well as auditing access to information. And even that is something most e-health providers would do anyway.

Desert norm

At the University of Arizona Medical Center in Tucson, HIPAA Program Manager Patti Redding finds that HIPAA collaboration begins at home. "What's really difficult is that we're an academic medical center that requires a high level of collaboration before you even go outside the walls. For example, as a first step I'll be collaborating with the college of medicine," she says.

That hasn't stopped the medical center from joining HIPAA efforts on both the state and national level, however. Late last year, Redding joined a statewide group of CIOs and other HIPAA compliance officers sponsored by the Arizona Hospital and Healthcare Association. The group decided to split into separate groups for transactions and security/privacy.

On a national level, the medical center is participating with WEDI in developing a HIPAA Security Policy Framework for academic medical centers that includes Yale, Mayo and Johns Hopkins. At the last meeting, the group analyzed each point in the security regulations from the standpoint of an academic medical center. "We have unique situations. Just like Y2K, you have to know what the best practices are for the diverse areas of research, education and residents," says Redding.

"Right now, I'm just building a team and a game plan," Redding says. "We did a security assessment and know what we have to do: take existing inventory; evaluate all software; make sure we have an audit trail, firewalls and security hardware in place; add and modify policies. The transaction piece is huge—evaluating EDI, talking with payers, evaluating EDI files and claims."

National heartbeat

She acknowledges the value of collaborating on HIPAA. "Our big thing is keeping in tune with the national heartbeat."

Fletcher Allen Health Care in Burlington, Vt., is working on or has completed major evaluations of the various facets of HIPAA, and is part of several national organizations that provide HIPAA support. As by far the largest healthcare provider in Vermont, Fletcher Allen lacks comparable local peers and finds greater value pursuing collaborative efforts on a national rather than regional basis. Fletcher Allen's legal team is working with law firms around the country that provide HIPAA expertise.

"There are a lot of interpretations that can be made," says Blake Jensen, Fletcher Allen's CIO. "We need to determine what the expectations and requirements are for HIPAA. The key concern is whether we can get to a commonly agreed-to rationale for what it means."

Providers and HIPAA: First Steps in a Long Dance

With the publication last month of final federal regulations for HIPAA privacy standards, the 24-month compliance clock is ticking. How prepared are provider organizations? We asked the question of two HIPAA experts: Glen Lutz, Practice Director for HIPAA services at First Consulting Group; and Keith MacDonald, HIPAA expert in FCG's Emerging Practices research arm. Here's what they had to say:

"Organizations are coming up with a blended approach," says MacDonald. "Many of them cannot afford to fund new positions in the form of a privacy officer, so they're combining these new roles with those they may already have, like a medical records staff person. It might require 10% of that person's time to manage audit trails on the back end, for example, to comply with the privacy rule," he says.

It's difficult to estimate how much HIPAA will cost provider organizations because approaches vary. "The particular approach is not mandated," says MacDonald, "only the required end result." For example, HIPAA requires that an organization be able to inform patients about their privacy. This might mean posters, brochures or Web-based information. "You have to figure out how to make the translation as to what's most appropriate for your organization," he says.

Who leads the charge on HIPAA also varies from provider to provider. In one, risk-management handles compliance and reports to the CEO. In another, that same function reports to finance. "Mostly it depends on who takes the initiative in the organization," says MacDonald, noting that both examples are fairly effective and lie outside the CIO's span of responsibility.

Fletcher Allen's director of business systems is working closely with local payers like Blue Cross and Aetna to develop HIPAA-compliant standards for electronic funds transfers. But Jensen's major concern remains establishing a benchmark in his own mind before backing any particular HIPAA strategy. "You have to understand what you agree with and don't agree with. The cost of implementing HIPAA will be huge. I want to know enough to be able to push back. I want to make sure I'm riding the high ground but not the mountain peaks."

Once that ground is established, Jensen is open to collaborating with other healthcare organizations to explore technologies, procedures and methodologies to comply with HIPAA. "The need to act is important, but we need to understand where we're going. The healthcare industry can't afford something that's six or seven times the cost of Y2K."

Why HIPAA implementation should be collaborative

It makes good sense for providers and health plans to participate in a collaborative effort to standardize transactions, especially the HIPAA ones, according to Bill Campbell of VIA Consulting in Bellevue, Wash., who is helping facilitate HIPAA collaboration.

His perspective incorporates "transaction" thinking and "solution" thinking. Transaction thinking focuses strictly on being HIPAA compliant—"Did we implement the transaction in a manner that is consistent with the regulations?" Solution thinking focuses on adoption and use by providers—"Did we implement the transaction and make it available in a manner that makes good business sense and that will encourage broad use by the provider market?"

Campbell's rationale for participation in a collaborative effort:

Consistent implementation increases provider usage, which justifies investments

- The end result of a collaborative effort will be more consistent implementation of transactions (solutions) across providers and health plans. Hopefully, consistency will increase the use of electronic commerce by providers, which justifies the investments that they and health plans will make in this area.

The HIPAA Implementation Guide doesn't have all the answers

- WEDI has published a HIPAA Implementation Guide that is quite helpful. However, it doesn't provide answers to all of the questions that arise when conducting a transaction. Each transaction guide defines all possible data elements and talks about "what data element goes where" within the transaction. Providers and health plans still need to agree upon what information they will actually put into the transaction and what it means once it's put there.

- Transaction-specific decisions that must be made by providers and health plans and that are not clearly addressed in the HIPPA Implementation Guide include:

Dot-commed health plan

Health plans tend to be more creative and proactive. A case in point: Harvard Pilgrim, which has set its goal to become a Net-enabled health plan. It became the beta site for an outside consultant to develop CD-ROM-based software to help its affiliated physicians meet HIPAA-compliant EDI objectives. The software helps physician offices exchange HIPAA-related payer information more readily with Harvard Pilgrim. In exchange, the consultant is free to sell the software to other plans.

According to MacDonald, Scottsdale Institute members tend to be more sophisticated than most healthcare delivery systems, which are taking a basic compliance approach, determining what they need to do just to comply. "They don't have the money or wherewithal for more comprehensive or strategic schemes," MacDonald says.

"What they're spending just on assessment is in the five or six-figure range. Health plans are spending a lot more—a quarter-million dollars and up," says MacDonald, who adds that, in contrast, many providers have only $50,000 to spend. Such conservatism reflects distrust on the part of providers who fear that HIPAA may be another hyped issue not unlike Y2K.

MacDonald offers these tips to consider in relation to other potential IT projects: "We recommend that if you're working on a project already or installing a new system, make sure you have audit trails and access control mechanisms. And if you find you lack a disaster recovery plan, you might be able to justify such a project under HIPAA."

What most of the world wants

Lutz sees provider organizations moving cautiously toward compliance. "Until the recent release of the privacy regulations, most provider organizations were focused on transaction sets and security." They need:

- Strategic planning
- "Gap analysis"—how an organization compares to peers
- Budgets for 2001 looking to complete tactical planning
- Education

"The health delivery market is still in the assessment and education/awareness phases. Very few are in remediation. Only those who have embraced e-health, with its associated need to address security and privacy and build a network infrastructure, are implementing HIPAA solutions," says Lutz.

"Most of the world wants to achieve basic HIPAA compliance, while a smaller percentage wants competitive advantage," he says. Lutz estimates that about 30% of HIPAA costs relate to IT. The rest goes to policies, procedures, and business-partner relationships. Still, many organizations mistakenly view HIPAA as an IT problem and, while CIOs are not necessarily a wrong choice to lead the HIPAA effort, to tackle HIPAA strictly as an IT initiative is a prescription for failure, according to Lutz.

Lutz sees a resurgence in regional and national initiatives (see main text) to organize players in the healthcare market not unlike the CHIN—and it's a much-needed development.

What information will each health plan actually include in the transaction?

- For the benefit transaction, what type of information and level of detail will be implemented in the transaction?
- For the referral-prior authorization transaction, what is the minimum set of information that must be supplied by the provider? What is the minimum set of information that will be returned by the plan, and in what time frame?
- For the claims status transaction, will status information be available for EDI and paper claims that were rejected?

Will the meaning of the information be consistent across health plans?

- For the benefit transaction, what benefit descriptions will be used and will they be standardized across plans?
- For the referral-prior authorization transaction, will the patients submitted by a provider match patients in a plan's system?
- For the claims status transaction, will statuses and reasons for rejection be standardized across plans?

Which transaction segments should be used, when should they be used and how should they be assembled for the predominant business scenarios?

As an example, the HIPAA Implementation Guide allows for a patient's eligibility to be associated with a product line, a clinic, a PCP and/or a particular benefit. These relationships are defined in data segments that can be assembled in different ways. How segments are built depends upon business scenarios—managed care, non-managed care, out-of-network contract. The guide does not discuss every possible business scenario. If a consistent solution is to be implemented across different business scenarios, conventions need to be agreed upon to make sure all health plans do it the same way.

The HIPAA Implementation Guide only addresses how a transaction is structured; it doesn't address broader issues such as security and workflow. In order to implement solutions, as opposed to just transactions, providers and health plans need to consider:

How will security be implemented across the community so that the health plan knows what provider is accessing their information?

- How will providers be registered?
- What type of electronic credential will be used?

How will the transaction solution be made available to providers and how will they interact with it?

- Does the transaction automate enough of the workflow process to make it worthwhile for providers to use it?
- Will providers use a browser interface or will the transaction be integrated into the practice management system or hospital information system?
- Will health plans distribute information through an intermediary?

Results can be achieved more quickly and cheaply as a group

- Staff from providers and health plans will move through a learning-design process to understand each transaction and to standardize its implementation. A group can do this more cheaply and quickly than an individual.
- Provider and health plan staff can share knowledge about what the transaction means and the best way to implement it.
- Peer pressure and an independent facilitator tend to keep providers and health plans engaged and on track, reducing the likelihood that the standardization effort will be delayed by changes in internal priorities.
- The costs of education and facilitation can be shared.
- Working together, providers and health plans can leverage their conventions across a region and may be able to influence national efforts.

HIPAA spawns communities of collaboration

Plenty of others seem to agree on the value of cooperation around HIPAA, which, like few issues, brings diverse elements of the healthcare industry together. From the Pacific Northwest to New England and from the Midwest to the Southwest, collaborative efforts to comply with HIPAA have proliferated.

"The national SNIP effort is sorely needed," says Maria Ward, a senior HIPAA consultant at First Consulting Group. "A lot of regional activities were taking place around EDI long before HIPAA, and some before SNIP. People said why not take advantage of those efforts. Have them filter up into the national initiative," she says, adding, "It's a huge task to comply with HIPAA in just two years' time. The value of doing it at the regional level is that it's not just an educational effort, we're talking about the sending and receiving of data with trading partners."

Many of those trading partners are sitting at the same table for the first time.

In Washington state, for example, the four largest health plans have joined together with the Washington State Hospital Association and the Washington State Medical Association to develop HIPAA solutions under the prosaic name of the Network Advisory Group Process.

"The market's driving this one," says consultant Campbell. "Everybody is doing their own project, but the solutions are harmonized. We get agreement on what will be built, so that all the individual proprietary pieces will fit together once they are implemented."

Making it look the same

The group agrees upon requirements, standards and conventions for automating HIPAA transactions. Their focus is not only information formatting standards, but how that information will be made available to providers. Standard, HIPAA-compliant eligibility solutions have been implemented by each of the four health plans. Health plans and providers are now working toward standardized claims, status, referral and benefits transactions.

"A provider can go up to a PC and get eligibility information from any one of four payers. It all looks the same to the provider, regardless of the health plan. Behind the scenes, each health plan has developed their own interface to their own system."

Massive rollout

"HIPAA requires an absolutely massive rollout: one million providers and 20,000 to 30,000 payer organizations need to comply. The real issue is how do you get everybody organized to share electronic information? We're starting to see many CHINs return because collaboration on a regional level is critical. A single provider may deal with 10 to 20 payer organizations. How do you work with each of them and still meet the compliance deadline?" asks Lutz, who acknowledges there are key differences between traditional CHINs and the newly emerging collaboratives.

Says Lutz, "The CHINs of old were focused more on hard-wires and infrastructure, the physical network. The new ones ask, 'How are we going to exchange data?' Most people don't care about the infrastructure. The new ones are more focused, with a defined purpose."

"A lot of regional activities were taking place around EDI long before HIPAA, and some before SNIP. People said why not take advantage of those efforts."

For every transaction set, WEDI has developed a HIPAA Implementation Guide. The Washington advisory group has developed a document that addresses five basic questions not covered by the guide. (See **"Why HIPAA implementation should be collaborative"** above.)

Next door in Oregon, the Oregon Medical Association HIPAA Forum has created three committees: The implementation committee will study privacy best practices and policies, review related Oregon law and make recommendations. The security committee will develop consistent security policies, define relevant staff roles and identify encryption technology that can be used when two organizations need to share data. A data set committee will establish transaction standards.

"In practical terms, I don't know how you can get a community HIPAA compliant without collaborating."

HIPAA happens in Pennsylvania

"In practical terms, I don't know how you can get a community HIPAA compliant without collaborating," says John R. Christiansen, chair of the group's security committee and co-chair of the planning committee for the Washington State HIPAA Readiness Forum, yet another Pacific Northwest collaborative.

"If you don't have a community- and market-based, regional effort, then what you get are inconsistent policies from plans thrown over the transom," he says, adding, "CHINs didn't happen, but the concept is still valid. HIPAA is forcing a lot of uniformity into the system in terms of claims processing and in adoption of computer systems."

"If you don't have a community- and market-based, regional effort, then what you get are inconsistent policies from plans thrown over the transom."

Meanwhile, a veteran of the CHIN movement is helping lead a major community-based collaborative effort in Pennsylvania. "There are going to be a lot of advantages to having regional collaboratives as opposed to individual provider or insurer efforts," says Martin Ciccocioppo, VP for research at the Hospital and Health System Association of Pennsylvania in Harrisburg. He sits on the board of the e Pennsylvania Alliance (ePA), a collaborative of the Pennsylvania Information Highway (PIHC.org) that reaches across education, health and business to find common solutions in the information age.

"ePA is a neutral table for various interests in healthcare to work out differences relative to HIPAA and provide for better coordination across system synergies," he says. The group includes vendors, providers, physicians, payers and the government.

▲

Mark your calendar…

Annual Membership Conference
April 4-6, 2001

Camelback Inn • Scottsdale, AZ

Program and registration materials will be on your desk soon!