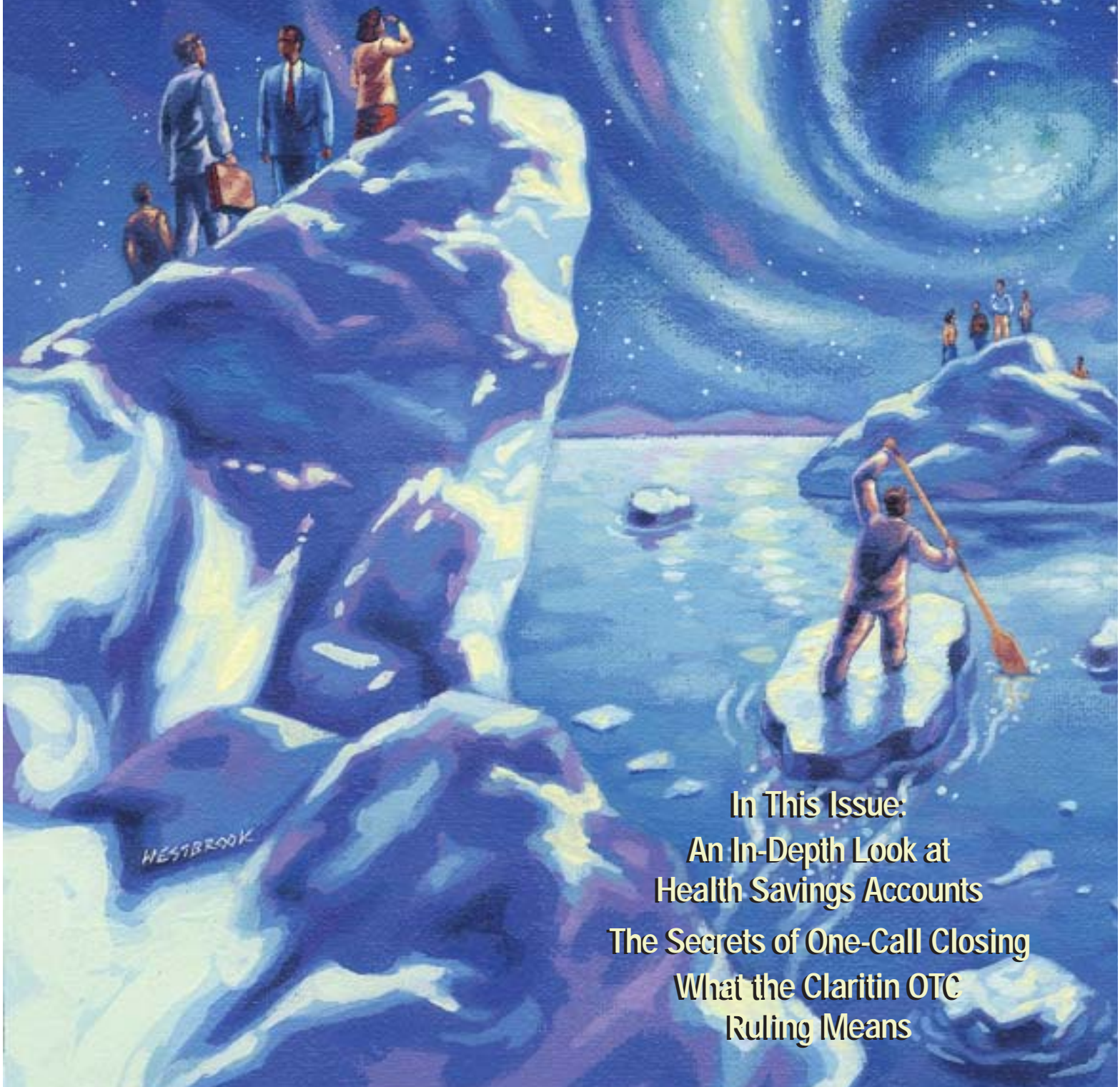


January 2003

www.nahu.org

HIU

HEALTH INSURANCE UNDERWRITER

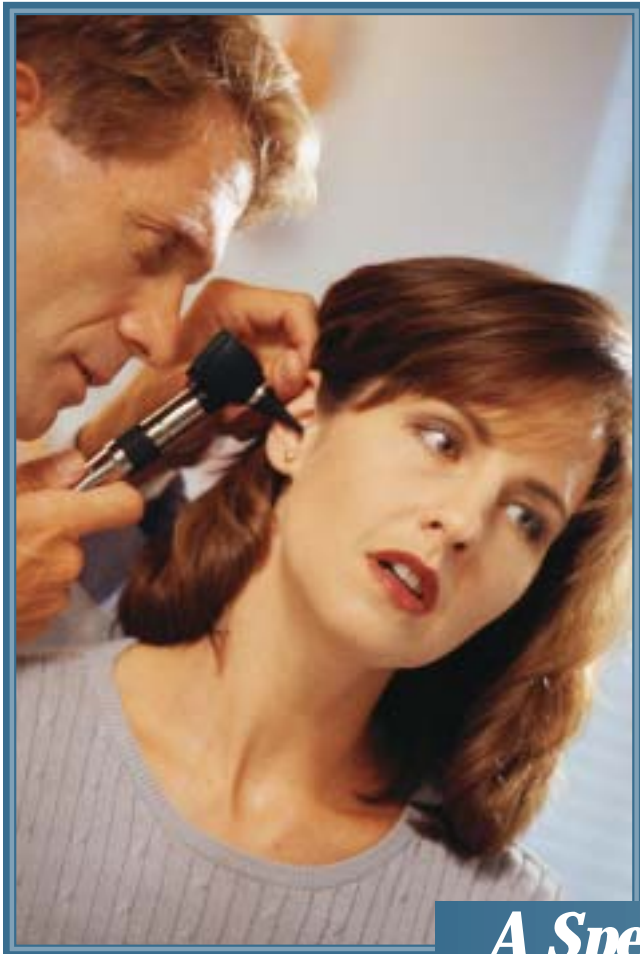


WESTBROOK

In This Issue:
**An In-Depth Look at
Health Savings Accounts**
The Secrets of One-Call Closing
**What the Claritin OTC
Ruling Means**

Implementing

HIPAA



by Dirk F. Niles
Co-founder, HIPAAAnswers
Eden Prairie, MN

HIPAA Administrative Simplification Rules comprise an incoming wave of regulations and requirements engulfing health care in a slowly rising tide of compliance-related action. For an update on compliance progress, here is a report from those on the frontlines of the compliance effort.

A Special Report from the Field

Quick Review

The HIPAA Administrative Simplification Rules were passed as part of the Health Insurance Portability and Accountability Act of 1996. The Administrative Simplification portion of HIPAA gives the Department of Health and Human Services (HHS) the authority to draft and implement rules for privacy, security, transactions, code sets and identifiers. HIPAA applies to three types of "covered entities:" 1) health plans, 2) health care clearing-houses and 3) health care providers who participate in the electronic transactions described by the rule. The compliance date for the Transaction and Code Set Rule was

October 15, 2002, for all covered entities except small health plans, although a one-year extension was offered until October 15, 2003. The compliance date for the Privacy Rule is April 14, 2003, for all covered entities except small health plans, who have until April 14, 2004. The only finalized rule for identifiers is for the employer identifier, which has a compliance date of July 30, 2004 (August 1, 2005, for small health plans). The Security Rule was not finalized as of this writing.

The Privacy Rule is currently of greatest concern to most covered entities, since most of them must comply with the rule by April 14, 2003. Under the Privacy Rule, cov-

ered entities must have in place policies and procedures describing the allowable uses and disclosures of individually identifiable health information. They are also required to "establish and maintain reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity, confidentiality and availability of the information."

These safeguards also extend to the covered entity's "business associates," or organizations that perform a service for a covered entity and receive or disclose individually identifiable health information in the process of performing the service. Covered entities are obligated to enter into written contracts with their business associ-

ates to receive written assurances that the business associate will safeguard the information as stringently as the covered entity and not misuse or disclose the information in violation of the Privacy Rule.

Summary of HIPAA's Benefits

Although perceived by some as just a large administrative burden, HIPAA was designed with several laudable goals in mind. The regulators anticipated several benefits from a health care system that achieves full compliance under HIPAA, such as:

- Improved faith and trust in the health care system.
- Greater likelihood that patients will seek more frequent and earlier encounters in the case of potentially expensive conditions, thus reducing health care costs.
- A national system of standards, rather than a patchwork of overlapping and inconsistent state laws.
- Reduced risk of unauthorized or inadvertent disclosure of health information.
- Cost savings due to elimination of redundant standards for common health care transactions.
- Improved billing cycle times for providers due to simplification of transaction standards, leading to reductions in claims submission errors and rework.
- Reduction in legal liability for covered entities due to lower probability of privacy breaches.

The Status of Current Compliance Efforts

Growing pains are likely whenever a major change in processes and strategies is required within an industry. However, even after years of meeting the variety of requirements from various regulatory agencies, health insurance companies and Medicare/Medicaid, complying with the HIPAA requirements is proving more than a little painful for most covered entities. For those in the health care market, there are many significant issues to overcome.

While most small to mid-size organizations have only recently start-

ed compliance work, common challenges, preferred compliance options and market trends are emerging.

Common Compliance Challenges

Challenge #1: *Understanding who needs to comply and the urgency of "when."*

As stated earlier, HIPAA applies to all health plans, all health care clearinghouses and all health care providers who send or receive electronic transactions. Health care providers, regardless of size, had to comply with the Transactions and Code Sets Rule by October 15, 2002, unless they received a one-year extension. They must also comply with the Privacy Rule by April 14, 2003. No extensions are available for the Privacy Rule. (Health care clearinghouses have the same compliance dates.)

Most providers are aware of their obligations under HIPAA, but many health plans are not. Their compliance dates are the same as those for health care providers unless they are a "small" health plan. A small health plan is one with less than \$5 million in annual premiums or less than \$5 million in claims paid. Small health plans have until October 15, 2003, to comply with the Transaction and Code Sets Rule and April 14, 2004, to comply with the Privacy Rule. Many health plans—especially group health plans sponsored by employers—do not understand the nature of their HIPAA obligations, and those who do have made only limited strides toward compliance.

Many business associates are also unclear about their obligations under HIPAA. The Privacy Rule defines the term very broadly to include any individual or organization that receives or uses PHI (protected health information) in the process of performing a service for a covered entity. This definition is bound to include most accountants, lawyers, actuaries, IT vendors, billing services, brokers, agents, third-party administrators, claims repricing organizations and others who have access to individually identifiable health information.

Covered entities are generally required to have valid business

associate agreements executed by the date they must comply with the Privacy Rule, but HHS has granted an extension for contracts that were in effect as of October 14, 2002, and are not modified between this date and April 14, 2003. These "grandfather" contracts, along with "auto-renew" contracts that are not modified during this period, do not need to comply with the requirements of business associate contracts until April 14, 2004. Although this extension appears to give covered entities some breathing room, the amount of leeway is actually rather small considering the amount of time necessary to negotiate business associate contracts. Many covered entities like to include specific indemnification language in their business associate contracts to protect the covered entity from liability in case of improper or inadvertent disclosure of health information by the business associate. This can lead to a protracted negotiations process that often involves the exchange of several drafts of the contract over several weeks or months. Covered entities with a large number of business associates should be aware of the potential complexity of these agreements in terms of time and resource requirements.

Challenge #2: *Understanding the massive scope of HIPAA remediation.*

Every covered entity's compliance activities are unique. Due to the large number of variables and dearth of compliance status results reporting, no Y2K-like formula exists to predict the amount of effort that an entity will expend on compliance.

Cheryl Jones thought her clinic was prepared to tackle HIPAA, but as the enormity of the task became apparent, it did not take long before her compliance committee knew it needed help.

"We were totally overwhelmed by the entire process," said Jones, the Director of Health Information for the Mankato Clinic, located about 75 miles southwest of Minneapolis. "We had no idea which direction to turn. The money involved in this is huge, as is the time commitment and the training needed," she said.

Challenge #3: *Identifying exactly what to do.*

A problem for many has been determining exactly what they should do—no more and no less. Articles and seminars can help in a general manner, but once you sit down and begin to work on your own organization, you realize there are many unknowns.

Jones had done everything right for an organization of her clinic's size, with more than 90 doctors in many specialties working out of six locations. The clinic's HIPAA compliance team included clinical directors and representatives from the lab, the compliance office, risk management and revenue management.

"In even outlining how to get started, we were banging our heads on the wall trying to figure out how to do this in a timely manner."

Challenge #4: *Making compliance as easy as possible.*

Compliance is a big job, requiring a structured approach. Some appropriate help will be needed. In reality, most people do not want HIPAA to disappear; they would just like it to be easier to understand.

Barbara Daiker is the administrator for Northwest Eye Physicians of Maple Grove, Minnesota, a practice with 14 ophthalmologists and four optometrists. They have eight locations in Minneapolis. "When we first started going through the HIPAA compliance process, it was like learning a whole new language," Daiker said.

Peg Feaski, regional vice president for Minneapolis' Center for Diagnostic Imaging (CDI), said her company looked at attorneys as well as big and small consulting firms before considering Web-based tools. CDI provides outpatient diagnostic imaging at 21 centers in five states with about 20 staff physicians.

"Anybody who goes through the HIPAA regulations could make a full-time job of reworking everything their organization is about," she said. "We needed a common sense approach to break the task down into manageable bits so it doesn't feel like you're solving world hunger."

Challenge #5: *Figuring out how to fit HIPAA into your schedule.*

Said Jones, "Just trying to keep our clinic operating is a full-time job." Daiker said the group was looking for a flexible way to work on HIPAA issues when employees had downtime. "There was no way we could spend our time researching, attending seminars and figuring it out ourselves. We have lots of work just to keep our clinic working. There wasn't any way to disengage from day-to-day activities. I suspect many clinics like ours don't have extra resources," Daiker said. "We have two people working on HIPAA. Our business manager probably spends about two percent of work time on HIPAA. I needed a tool I could squeeze in between other things."

Challenge #6: *Determining the most cost-effective way to comply.*

For small and mid-size companies, the struggle is to find an affordable way to comply.

According to Daiker, "If the administrator doesn't have two percent of their time to commit to it, they are going to have to go to a consultant. If they do it without any help, they're going to have to spend 25 percent of their time on it."

Feaski said, "There's a wide range of resources out there. We wanted to do most of the work ourselves so we would learn and reduce our risk for complying with the regulations."

Outside expertise is rarely cheap. "For a consultant to come in, I haven't heard anything less than \$10,000."

Common Compliance Options

Dawn Lunde began weighing the pros and cons for a variety of approaches to compliance two years ago. Lunde's employer, Minnesota Healthcare Network, provides management functions for doctors and health organizations in Minnesota and western Wisconsin. As director of network services, she took the lead in figuring out what the group's role

would be in helping the network's 410 affiliated doctors in 36 health care organization operating 60 locations.

"Our groups range in size from one physician to about 25," she said. "Right away we knew we had a quandary on our hands. We determined early on our role would be to find resources they could choose from and coordinate educational sessions. We're not doing the work for them."

So Lunde began researching the options. She put together education sessions for network affiliates which identified what they could expect from the four most common approaches to HIPAA compliance:

- Hire an attorney. Lawyers interpret regulations and advise clients on their legal responsibilities, so it seems natural to look first for legal advice. Firms with real expertise in HIPAA can be a tremendous resource, but those are often the big law firms that come with big fees. Since cost is a chief concern for small or mid-size organizations, many find themselves ruling attorneys out for that reason alone. Others have found themselves counterproductively explaining the regulations to the attorneys in their initial meetings.

- Do it yourself. For organizations that have the right expertise and can find a way to break key personnel loose from their regular duties to focus on HIPAA compliance, this is an attractive option, and often much cheaper than lawyers or consultants. A benefit to this approach is it creates in-house experts in HIPAA regulation who can be relied upon in the future. But the time investment can be gigantic. Just reading and interpreting the regulations is a huge job. Without any outside guidance, creating a compliance plan can be daunting. Mistakes can result in inconsistent interpretation of the regulations, which might slow the process or bring higher costs later on. Staff at smaller organizations also may not have the background or skills to conduct a gap analysis or to develop project management work plans.

- Hire a consultant. Expert guidance can help an organization focus on the important areas and mundane

time-consuming tasks can be outsourced. However, the consultant's perspective of the regulation likely will dominate the plan, and achieving compliance will still require time and effort from within the organization. The biggest problem with this approach is, again, the potentially high cost. Also, if the consultant is asked to do most of the work, the organization may be left without internal experts who understand the regulations.

- Purchase software or a Web product. Many small and mid-size companies are finding this to be their

Because so many of their clients might be slow adopters, insurance agents and brokers do their clients a service by raising the issue and offering advice. For some brokers, HIPAA compliance tools and solutions could be another product they offer their clients.

best option. Most products have some sort of education section. Many also include the original legislation and update their systems as regulations change. The better packages offer step-by-step instruction designed for the busy HIPAA project manager. The software or Web service approach is less costly than consulting fees and less time-consuming than tackling compliance entirely on your own. The best Web tools act as a "consultant in a box," much like popular tax preparation software, and ask users a series of questions to assess their needs. Ultimately these solutions produce documents customized to meet the unique needs of the covered entity. Web tools still require employee time to execute and they may have to be customized to the organization. But as with the do-it-yourself approach, employees will become experts in HIPAA compliance. For top products, the results are tailor-made—as if a consultant had done the work. (See sidebar)

Ultimately, Lunde's, Daiker's, Feaski's and Jones' organizations all

picked a Web-based compliance service: HIPAAAnswers.

Details, Results and Trends

HIPAA compliance has become a little like the weather—a lot more people talk about it than do something about it. With the threat of storm clouds gathering on the horizon, relatively few are taking the precautions needed to avoid getting soaked.

As we have contacted potential clients, one of the most common statements we hear is, essentially, "We have HIPAA under control."

Certainly some do, and others are saying that merely because they are too busy to talk to salespeople. But others willing to converse a few minutes have explained what they mean by "under control"—and wind up surprised at just how out-of-control they actually are once they better understand the full implications of the HIPAA regulations.

Other potential clients have reported that they don't intend to comply. We understand how they might feel about having to tackle a difficult and unfunded mandate, but this response is naive. They are putting their organization at risk.

Research bears out the foot-dragging organizations have displayed toward HIPAA compliance:

- 550,000 out of approximately 2,000,000 covered entities applied for extension. It's doubtful the rest did not apply because they are already compliant. More likely, they are in a state of noncompliance.

- According to the Centers for Medicare & Medicaid Services (CMS), unprepared facilities that missed the

October 15 deadline to apply for the Transaction and Code Set Rule compliance extension should comply as soon as possible, and prepare for possible complaints.

- CMS officials say they will not actively pursue the more than 1 million covered entities that are not compliant with the Transaction and Code Set Rule and which did not apply for the deadline extension. They may not have to pay fines at first, but should be prepared to submit a corrective action plan in the event a complaint is filed against them.

- Fines for noncompliance can be as high as \$100 per offense, with a maximum of \$25,000 per year, but CMS has said enforcement will be complaint-driven.

- The American Medical Association is urging all physicians who didn't file for the extension to become compliant as soon as possible.

- A survey conducted in early July by Phoenix Health Systems reported only five percent of providers and payers had actually completed Privacy and Transactions remediation.

- The survey also reports covered entities are focusing mainly on Privacy and Transactions compliance; Security initiatives are moving more slowly, despite Privacy Rule mandates for strong security measures to protect confidentiality.

- Across the industry, HIPAA budgets are generally higher for 2003 than for 2002.

What Should be Done Next?

As a professional working in the health care market, here are some specific actions to take. Given the status of compliance efforts to date, you may find you can provide valuable assistance to your organization and those with whom you interact.

Get to know some of HIPAA's major concepts. Understanding some basic facts about HIPAA will make progress faster. These facts include:

Protected health information (PHI)—PHI is the nut within the shell that is the Privacy Rule. PHI is, simply, individually identifiable patient health

Evaluating Web Tools

Software companies, consultants and others are now dipping their toes into the HIPAA Web-based tools market. Many firms are using simple software to sell their higher-priced services while other applications focus on eliminating or dramatically reducing the need for expensive consulting assistance.

Robert Tennant, government affairs manager of the Medical Group Management Association and co-chair of the Workgroup for Electronic Data Interchange's Strategic National Implementation Process, said many organizations have looked to Web-based programs after the cost of consulting scared them off.

"It's much cheaper than hiring a consultant and tells you all you need to know," he said.

To choose a HIPAA-compliance Web tool that makes sense for an organization, a good place to start is by asking colleagues what worked for them, Tennant said, and to seek advice from professional organizations.

"We have encouraged our members to network with their colleagues," he said. "They can learn a lot from how other practices are doing things. You want to adopt best practices within the industry and not do a lot less or a lot more than what is required."

Tennant said its best to get advice from someone trustworthy who understands HIPAA.

Gail Sausser, chairwoman of the HIPAA task force for the Health Care Financial Management Association, warns that organizations should avoid companies that don't usually work in health care or that promise to solve all HIPAA problems.

Among the issues experts suggest organizations consider:

- How easy to use is the service or application? Does it include definitions and help?
- Does the application include references to the original legislation, and the legislation itself, along with clear interpretations?
- What additional consulting services are available or required?
- How does the software address state-level pre-emption?
- Is application support and maintenance included?
- Does the software have several client references similar in size, scope and location to your organization?

Tennant advises organizations interested in Web tools or software solutions to educate themselves first. A good place to start is the Internet. WEDI's website has general information about HIPAA that can help.

Tennant suggests looking for programs that:

- Can modify content. "The rules are continually changing. You need a product that is flexible. If it's one-time purchase, you may not have that option. It's better to be on a subscription basis so you can get any modifications."
- Are not overpriced. "Ask yourself what makes the more expensive products better than the cheaper ones."
- Include templates. "They should include template forms so you don't have to reinvent the wheel. That will cut down a lot of staff time."
- Use language that is easy to understand. "Make sure the product is aimed at your level of understanding. If it's too technical, it may not be usable. Can you train clinical, clerical and administrative staff with it? Does it have that flexibility?"
- Provide gap analysis. "You need to get the lay of the land. How far away from compliance are you?"

information that is maintained in any format or media. The Privacy Regulation's purpose is to define appropriate use of this information and to impose guidelines to ensure that allowable usage standards are not violated.

Safeguarding PHI—The actual amount of text dedicated within the Privacy Rule to this specific topic is very limited, but its intent has broader implications. In short, covered entities are expected to take "reasonable steps" to ensure that protected health information is not inappropriately used or disclosed.

However, the Privacy Rule cannot cover every aspect of an organization's business practices; this is why the concept of safeguarding should be constantly reconsidered. Should you lock that medical records file cabinet? The Privacy rule itself says nothing of the sort; but your understanding of the safeguarding principle likely will lead you to do so.

Preemption — Much of HIPAA is consistent with existing state laws, so many of the practices it introduces are not new. In most circumstances, HIPAA imposes tighter restrictions. Still, HIPAA does recognize that some states' laws are even more stringent than, and incompatible with, HIPAA. Where that is true, HIPAA generally requires that the state law take precedence...a concept known as preemption.

Understand What Compliance Looks Like — Once compliant, an organization will have created and implemented a set of policies, created and implemented procedures to reflect those policies, and provided appropriate training to all workforce members regarding their responsibilities for abiding by those policies and procedures. In addition, the organization will be able to support the standard versions of the electronic transactions that are appropriate for its type of organization.

These standards include the use of the appropriate code sets and identifiers. For example, health insurers and HMOs will need to be able to support the standards for electronic claims, claim status, referral and eligibility (among others). When the Security Rule becomes final, organizations will need to implement detailed administrative, physical and technical safeguards for all health information stored or maintained in electronic media.

Having documented policies, procedures and training is a formal require-

ment under HIPAA. If audited or otherwise asked to demonstrate that you are in compliance, you must have this information available in paper or electronic form.

In many cases, organizations will also combine their HIPAA-related practices with general policies and procedures already in place. The consolidated information will also need to account for state laws, which in some cases pre-empt HIPAA. Here, an attorney's assistance may be necessary.

Consider who in your personal and professional network should comply, and help them understand the issues. They may be fully funded or self-funded group health plans, HMOs, health insurance issuers, DMEs, pharmacies, home health providers, skilled nursing facilities, nursing homes, health care clearinghouses or any other type of covered entity.

Because so many of their clients might be slow adopters, insurance agents and brokers do their clients a service by raising the issue and offering advice. For some brokers, HIPAA compliance tools and solutions could be another product they offer their clients.

Sometimes agents or brokers act as an intermediary between a provider and a plan, in which case they too might be on the hook for HIPAA compliance.

Know how to approach compliance and what assistance is helpful (or not). The only way to tackle an initiative such as HIPAA is with a structured approach and some trusted assistance. These can be Web tools. (See sidebar.)

Polly Edwards, administrator of Burnsville Family Physicians, a suburban Minneapolis clinic with six physicians, took about an hour to determine her group's "covered entity" type. Using a Web service, this activity required no additional help from an attorney or consultant and yielded 60 HIPAA requirements deemed applicable to the clinic.

It also helps to know what DOESN'T work. Northwest Eye Physician's Barbara Daiker said she tried talking to the company's attorney about HIPAA compliance. "It was really expensive and I don't really know if they knew much more than we did. I told them everything," she said. "I spent 45 minutes with them and I got a \$1,800 bill. I told them, 'I'm not paying for that. You didn't teach me anything I hadn't already learned from our Web service.'"

Look for time- and money-saving efficiencies wherever you can. Polly Edwards found her original 60 requirements condensed into only 17 policies. For example, the 20 requirements regarding disclosures combined into a single "Disclosure Policy." Having information readily accessible is also necessary. Barb Daiker said, "It was helpful to have definitions in the Web tool so we could ask, 'What does this mean? Does it apply to us?' If we got stumped, we called or e-mailed the vendor and their experts got back to us."

If you must comply, complete a few simple requirements first. When administrators get their toes wet in the regulations and start making progress toward compliance, the job will feel less daunting. As an example, consider HIPAA's complaint requirement.

Most service organizations have a simple policy in place that describes how complaints will be received and processed. HIPAA adds very little substance. It imposes formalities, like making sure the complaint policy and procedures are written down, ensuring complaint receipt and resolution are documented; and making sure staff is trained to process complaints and can explain the process to those who want to complain.

By incorporating this information into the existing complaint policy and procedures, an organization completes a HIPAA requirement. During this process, it will also assign—and document the assignment of—a Complaint

Contact. As a result, a second HIPAA requirement is completed. The organization cannot go much further without assigning—and documenting the assignment of—a Privacy Official responsible for document creation and policy enforcement. That would be a third HIPAA requirement completed.

Administrators at each covered entity will have to learn the general requirements for documenting policies and procedures throughout that process. If they document this information in a policy template, that completes yet another HIPAA requirement.

Summary

HIPAA represents an opportunity for progress throughout the entire health care market—providers, health plans, clearinghouses, insurance agents and brokers. The opportunity can be onerous and overwhelming for entities that try to go it alone and can be costly for entities who hire expensive outside help. One approach that makes sense for any covered entity is online assistance such as that offered by HIPAAAnswers. Agents and brokers familiar with such products are in a position to both advise their health plan clients as well as create a business opportunity by becoming a distributor of such solutions. They can serve their clients while generating a new source of revenue. ■

Dirk F. Niles has 15 years of health care experience in technology sales and marketing, software development and e-commerce strategy. He has worked with Express Scripts, CIGNA Behavioral Health, BlueCross/ BlueShield of Minnesota, PriceWaterhouse Coopers and others. Dirk graduated from the University of Minnesota with a self-designed BS degree focused on optimizing technology in health care. He can be reached at dirk_niles@hipaanswers.com.