

Online, on Message, on Duty:

Privacy Experts Share
Their Challenges

An AHIMA Roundtable

April 2008

As more providers make the transition from paper to electronic health records, the healthcare industry's understanding of privacy and security issues related to electronic data is maturing as well. However, while the information age promises more efficient and better care, it also poses a particular set of challenges, as evidenced by headlines of security breaches and privacy violations. Just last month, the National Institutes of Health announced that a government laptop computer containing sensitive medical information on 2,500 patients enrolled in one of its studies had been stolen, and the UCLA Medical Center in Los Angeles announced that it was firing at least 13 employees and disciplining six others for peeking into entertainer Britney Spears' medical records without cause while she was hospitalized in its psychiatric unit.

Even as security and privacy breaches hit the news, progress is being made rapidly toward regional and even national transfer of electronic health information through a network of

networks. This, too, has presented particular challenges, such as inconsistent state laws governing the release and transmittal of medical records.

Providers have guidance on privacy and security matters through the privacy and security regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), implemented in 2003 and 2005, respectively. Meanwhile, enforcement is carried out by several entities, such as the Office for Civil Rights, which enforces privacy rights and standards, the Office of Inspector General, which started HIPAA compliance audits for security in 2007, and the Centers for Medicare and Medicaid Services (CMS), which announced in January that it has hired PriceWaterhouseCoopers to conduct compliance reviews of security programs.

In acknowledgment of AHIMA's Health Information Privacy and Security Week, April 13–19, AHIMA spoke with four privacy experts to discuss these issues and how the industry can best address them. Their opinions are diverse, but some common themes emerge:

- To prevent breaches of the privacy of health information, education and attention to issues of access are critical
- Healthcare privacy officers continue to work to resolve perennial challenges such as differing laws and misinformation about HIPAA in addition to emerging issues such as medical identity theft and portable device security
- Preparation and a proactive approach are recommended in light of the development of CMS's program to investigate alleged breaches
- To ensure that an organization's privacy and security functions work together effectively, an approach that combines communication and collaboration is key

Healthcare privacy issues have appeared in the news fairly often during the past year, including breaches of the medical records of celebrities such as George Clooney and Britney Spears, and systemic lapses in privacy and security in which entire databases have been compromised. Given the frequency of these events, are there common practices in the industry that need to change?

Husher: I don't know that practices need to change or new ones need to be adopted, but I think in our day-to-day training we need to keep in front of people the sensitivity of the information they're dealing with and the importance of keeping private and confidential information private and confidential. We can implement changes all day long but if people don't practice good behaviors we'll never accomplish what is needed. I think we need to keep in front of our employees that they are dealing with highly confidential information that doesn't belong to them. They need to be trained and know that we will follow our sanction policies to resolve security breaches resulting from activities like not storing laptops appropriately or accessing records they have no need to see. It all comes back to basic employee behavior.

Icenogle: The biggest problem with the advent of EMR systems is the failure of entities to institute

proper controls on the EMR and to understand what proper controls are. In the case of Britney Spears' records, the 13 people who accessed them inappropriately were fired. That shows two things: one, that the records were easy to access; and two, that it was easy to find out who accessed them. It illustrates both sides of the issue. On the one hand, it's easier to access an EHR than paper records [if access security is not in place]. On the other hand, because of log-in and audit features, it's possible to know every part of the record that was accessed, and by whom.

Another big issue is that people don't take simple steps to ensure the security of records. For instance, some of the incidents of mass release like those the Veterans Administration has experienced have occurred when normal security procedures weren't followed, such as not cleaning out hard drives when computers are being replaced. The HIPAA security regulations and AHIMA record protection standards together are creating a kind of standard of care, but the responsibility for privacy and security is still on the backs of individual institutions. I think it's hard to talk about an industry-wide approach because each institution is so different. Every system is different and security concerns are different for smaller organizations that are hardly ever on the Internet versus some of the national integrated delivery systems that have data constantly out on the Internet. That's the beauty of HIPAA; it requires each organization to look critically at its own systems.

Our participants included:



Jamie Husher, RHIA, CHPS, director of HIM and privacy officer, The Evangelical Lutheran Good Samaritan Society, Sioux Falls, SD

Daniel Icenogle, MD, JD, attorney, Icenogle & Associates, Readstown, WI



Wendy Mangin, MS, RHIA, AHIMA president and director of medical records and privacy officer, Good Samaritan Hospital, Vincennes, IN



Laurie Rinehart-Thompson, JD, RHIA, CHP, assistant professor of clinical allied medicine, The Ohio State University, Columbus, OH

Mangin: Here at Good Samaritan we've made a concerted effort to provide more organized education to all our staff, not just new hires. The breach of George Clooney's records is a perfect example which I cover in our new employee orientation when I talk about egregious breaches. I make the point that even if we're not taking care of famous people, it still is a very serious issue when protected health information is released inappropriately. We also talk with all employees throughout the year. During our annual education day we include privacy and security training along with things like infection control, fire safety, disaster training, etc. So part of it is raising awareness; it's something you constantly have to hit.

Another thing that all facilities, whether large or small can do, is to step up their auditing and increase the monitoring of employee access to protected health information. They also might consider more sophisticated access control, such as limiting access to patients currently on a nursing unit. At least they can look at audit trails and logs to see if there has been any inappropriate access. The public will, and has a right to, demand this.

Rinehart-Thompson: The lapses involving Britney Spears and George Clooney bring up the issue of whether facilities are giving too many people too much access to records. Organizations need to take a second look at who has access to what and across-the-board restrict access as much as possible without compromising patient care. Also, you can have employees sign agreements that they're not going to breach privacy and that there will be progressive penalties if they do, but we need to instill in people that they wouldn't want to access records inappropriately because it's not part of their value set. It's a culture change, and more of a values-based positive approach of respecting patient dignity rather than just punitive measures when violations occur.

Q *In your view, what are the greatest challenges involving healthcare privacy and security, and how should the industry address them?*

Husher: As we make the transition to EHR we are also using a variety of portable devices, and we need to make sure that protected health information on those devices is secure. We need to have good controls about who can download information to portable devices and make sure there is good technical control with the methods used to download and maintain that information.

Another concern is keeping up with differing federal and state privacy laws. It's still challenging to know all the state laws. The easiest solution would be one federal regulation that would pre-empt state laws. That would be the easiest thing for patients seeking healthcare across multiple locations, and it would be easiest on providers. As the world shrinks it's not uncommon for patients to live six months in one location and then go to another home for six months. Differing state laws impede getting needed information to healthcare providers, so I do think some federal initiative would be very helpful.

Icenogle: The biggest problem is financial. EHR and related security are tremendously expensive and require constant maintenance and re-evaluation. If an organization commits to an EHR, it is committing to a tremendously expensive process and has to spend money throughout the system. An EHR is not just hardware and software; it's also security and that tends to be ignored, but it's a commitment that has to be made.

Mangin: There is an absolute need for universal laws without pre-emption because pre-emption leads to misinterpretation of laws. Sometimes organizations use HIPAA as an "out" for policies that really are too restrictive, but it's probably due to a misinterpretation on their part. There also needs to be a HIPAA-compliant authorization form that is adopted nationally. We spend a lot of time looking over authorization forms [received from other entities] to

determine if they conform with HIPAA. Time spent doing that is time lost processing the information. Addressing those two things will break down barriers that exist today in releasing information.

We also need to better educate everyone on interpreting laws. For example, some facilities won't accept faxed authorizations. They say they must have a mailed authorization or an original authorization, but that slows the process of getting records, even though it's for patient care. Another example is redisclosure of records that came from other providers, when it's used for patient care. Some medical practices and facilities will not redisclose information. So there needs to be more education about good privacy practices and appropriate interpretation of HIPAA and other regulations.

Rinehart-Thompson: One of my big concerns involves personal health records. They're wonderful and there are more and more options for consumers in that regard. However, some of the organizations hosting PHRs are not covered entities, but vendors, and they're not subject to HIPAA. People don't realize if there is a breach in a PHR not operated by a covered entity they may not have the same protections and the host organization may not be held to the same standards as a covered health entity. Short of lobbying for changes in HIPAA, we need to educate the public that not all PHRs are alike, and what it means to use one sponsored by a covered entity versus a noncovered entity.

Medical identity theft is another growing concern, but I'm not sure how it will be sorted out. This, of course, is when someone creates a fictional health record using certain information from another person. The victim can be selected at random but can also be a family member, where one person has health insurance and the other doesn't. So the family member without it assumes the identity of their insured relative to receive medical treatment. The problem is, when the victim reports the fraud, existing laws are such that providers are required to protect all the information in the record, even though part of it belongs to the thief. So the victim is effectively prohibited from seeing his or her own record because it contains protected

information on two people. Beyond having good procedures to verify identity at the time of service, I'm not sure what the answer is to this, but it's something the industry needs to be thinking about.

I also think we need to look at the misinformation about HIPAA that's still out there. Providers are still using HIPAA as a shield to withhold information, and there's still an attitude that the records belong completely to the provider and they're very possessive of them. Obviously there is a need for more education, but the industry is so fragmented, unless patients take it upon themselves to complain I'm not sure what the best mechanism is to reach offenders. Perhaps we, as an industry, could suggest to CMS that review release of information procedures be a priority in their audits, because the sharing of information is in the interest of quality patient care.

As HIPAA enforcement by CMS and others is stepped up, how should organizations prepare and what can be done to mitigate any negative consequences should an audit not turn out well?¹

Husher: Preparation is the key. Most organizations would be well served to access a checklist CMS has published that indicates who may be interviewed and the documents and other information that may be requested.² They should use this to conduct an internal assessment and ask if their organization could meet the security standards. If they identify a gap where they're not in compliance and develop an action plan to get into compliance, they can point to that should CMS conduct an audit before they've been able to implement all of the action plan. CMS has also said that it will offer technical assistance to organizations not in compliance. In terms of any negative findings from an audit, regardless of how you feel about it, you need to accept whatever CMS says because at the end of the day, they're the people who have the enforcement role. Of course you can seek further clarification, but you have to act on their findings and act in a timely manner to respond.

Icenogle: The important thing is to document all decisions when you go through the process of determining the information systems used and the security procedures applied to them. That way, when CMS comes in and asks why your organization did things a certain way, you'll be able to tell them.

If you get dinged on something you have to take it seriously and be up front about it. If you're dinged and it becomes public, you could have a huge problem on your hands. In that case, as has been demonstrated in crisis communication situations across the board, you have to be open about the problem and how it will be corrected. Otherwise, there could be a crisis of confidence. If the public thinks its health information is vulnerable, it will create a bottom line problem for the organization, so you don't want to go there. You have to be open, forthright, and out in front of it. CMS will tell you what you need to fix. That's the easy part. The hard part is dealing with the public disclosure.

Mangin: Facilities should be proactive by conducting their own privacy and security audits and correcting any problems found. There are two things we've done at Good Samaritan in that regard. First, our security officer and I came up with privacy and security items that are included in the annual safety inspection of our organization. This way there's not a double work effort and we can identify issues efficiently through the safety inspection. One of the things on our checklist is determining whether protected health information has been disposed of improperly. We have a system using green bags where protected health information is disposed of more confidentially than regular office trash. We ask that any document containing PHI be placed in a green-bag container and the contents of these bags are shredded with an industrial-size shredder on site. Another is if the safety inspector sees any protected health information left unattended, such as charts being left out inappropriately. If any problems are found we give feedback to the appropriate department to correct whatever issues are identified.

Secondly, we've stepped up security access audits and shared them with managers and supervisors to rectify any problems. We already have privacy and security violation policies with different levels of violations and corresponding sanctions for each, but we've started picking up our monitoring activities to see who is accessing information, what is being accessed, how long it's being accessed and the like. It's pretty detailed. We do this in such a way that there's a division of labor. That's the only way to make it work, because otherwise there aren't enough resources. What happens is on a quarterly basis I have the information systems department run some queries for me. They e-mail the results and I sort them by department and employee and forward them to the appropriate department manager. We pick one week randomly, and it's done quarterly. It's up to the department managers to determine for their employees who did or didn't have the right to access the information they accessed.

When it comes to an actual CMS audit, you have to take action quickly to correct any problems found and be open and cooperative about it. Staff also has to be educated about it so that it doesn't happen again and then you can focus on prevention efforts to prevent any further occurrences.

Rinehart-Thompson: It comes down to preparation. The CMS audits are starting to look more like Joint Commission surveys, so we should take a lesson from those surveys. One thing is to do unannounced mock audits so that it's more realistic. You'll be able to see how the organization is responding and check whether policies and procedures are being followed. If there are known problem areas, then they should be a focus of the effort.

When CMS comes in, cooperation is the key. Of course you have to follow up on any areas of negative findings and check on a regular basis that correction plans are being adhered to, again, by doing surprise internal audits.

Health information security and privacy responsibilities often are divided between two people or departments in healthcare organizations, although their aims are similar. How can these two separate, but related, functions work together effectively?

Husher: Here at the Good Samaritan Society, I meet regularly with our information security officer. We discuss from both our perspectives what is going on in regards to privacy and security. We house our procedures together so there's a one-stop place for privacy and information security. The effort is really to blend the programs so to the end user we aren't really separate but equal. My information security counterpart and I have a good working relationship and we work closely on training, policies, and the like so that there's really a blended approach to compliance. For issues in my department, I try to look at things with an information security eye and when it's appropriate I bring in my information security colleague, and he does the same with me. Organizationally we report to different vice presidents, but because of our collaborative approach it really hasn't been a problem.

Icenogle: When EHRs were being implemented and HIPAA was first rolled out early on, there were questions about whether information technology people would be running the whole thing. That made health information people nervous, so for the most part privacy issues were put in the hands of health information people. It's difficult getting health information and information technology people on the same page at the same time because they're from different backgrounds and speak different languages. So how do you get them to work together? Organizations handle it in different ways. The main thing is to make sure that everyone is talking together.

Mangin: Different organizations are set up differently. If privacy and information security are separate, as they are here, the two people responsible need to work very closely together in their efforts towards compliance. When we were working on implementing the HIPAA privacy regulations, our information security officer was part of the team which I lead. Then I was part of his team when we implemented the security provisions.

We also try to collaborate whenever we can. For employee education, we worked together on developing an overview of privacy and security issues, and we trade off every other week in making the presentation for both new employee orientation and continuing education for existing employees. We have conversations about how to deal with real privacy and security issues and if an issue comes up we talk about how to deal with it so that it's handled in a consistent manner. If there is a new information system application, both of us are involved so we can address any privacy and security issues up front. Basically rather than being in two separate silos and not talking about issues we have a very strong collaborative relationship and we both report to the same individual.

Rinehart-Thompson: My first suggestion is to marry privacy and information security in some way so that they're in the same department or report to one person, preferably the top information officer. I've been in organizations where the information technology department thought it possessed the information because of the medium it's on. Putting both privacy and security under the same department will help address that.

Report compiled by Gina Rollins.

Notes

1. For a month-by-month overview of CMS's enforcement activities, see www.cms.hhs.gov/Enforcement/03_HIPAAEnforcementStatistics.asp#TopOfPage. See also the Office for Civil Rights (www.hhs.gov/ocr/hipaa) and the Office of Inspector General (<http://oig.hhs.gov>).
2. Department of Health and Human Services, Office of E-Health Standards and Services and the Centers for Medicaid and Medicare Services. "Sample-Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews." Available at www.cms.hhs.gov/Enforcement/Downloads/InformationRequestforComplianceReviews.pdf.

AHIMA is the premier association of health information management (HIM) professionals. AHIMA's 51,000 members are dedicated to the effective management of personal health information needed to deliver quality healthcare to the public. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning. To learn more about the association, go to www.ahima.org.

To raise public awareness about issues related to the privacy and security of health information, AHIMA sponsors its annual Health Information Privacy and Security Week, April 13–19, 2008. To learn more about AHIMA's Health Information Privacy and Security Week, go to www.ahima.org/hipsweek.

To ensure that its members meet professional standards of excellence, AHIMA issues credentials in health information management, coding, and healthcare privacy and security. Among AHIMA's credentials is

the Certified in Healthcare Privacy and Security (CHPS) certification which denotes advanced competency in designing, implementing, and administering comprehensive privacy and security protection programs in all types of healthcare environments and settings. To learn more about the CHPS credential, go to www.ahima.org/certification/chps.asp.

