On the Front Lines of Healthcare Privacy

An AHIMA Roundtable

What's on the Minds of Privacy and Security Officers Today

AHIMA
American Health Information Management Association®

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. For information about the association, go to www.ahima.org.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was a milestone in enabling patients to access their health records and in holding healthcare organizations to privacy and security standards. Most of the healthcare industry implemented the final HIPAA privacy rule in April 2003 and the final security regulation in April 2005. Yet in many ways HIPAA was just the beginning of an ongoing process to balance access to information with privacy and security concerns.

In addition, numerous states have enacted privacy and security regulations of their own, some of which have more stringent requirements than HIPAA. Technology has also come to the fore. Momentum has grown toward development of health information exchange, which will enable health information to be shared electronically, across geographies, with the goal of improving patient care and enhancing the efficiency of the care process. Technological advances also represent new challenges for those charged with managing health information, particularly in light of numerous high-profile security and privacy breaches.

All of these circumstances have affected the role of privacy officers in healthcare. On the eve of the fourth anniversary of implementation of the HIPAA privacy standards, AHIMA spoke with four privacy professionals about the changing privacy and security landscape and the role of privacy officer. They offer their views from the front lines of healthcare privacy and security, including:

- How privacy and security officers play a broader role than ever before in their organizations
- How their role has become more complex with the introduction of health information exchange and increased interest from the public
- Where challenges still exist in managing some HIPAA standards
- How challenges still remain with regard to educating consumers about their privacy rights

Our participants are:

- **Jana Chvatal**, CHPS, CIPP, CISA, manager, privacy and information security office, Texas Children's Hospital, Houston, TX
- **Nadia Fahim-Koster**, MBA, CHPS, CISSP, information privacy and security director, Gwinnett Health System, Lawrenceville, GA
- **John Gildersleeve**, CHPS, system privacy officer, Geisinger Health System, Danville, PA
- **Joan Kiel**, PhD, CHPS, HIPAA compliance officer, Duquesne University, Pittsburgh, PA

Q: How has the role of privacy officer shifted from an emphasis on HIPAA to a broader role?

Kiel: The privacy rule is one of 11 under HIPAA, and while the privacy and security rules are the umbrellas we operate under, as more rules come out we have to integrate them with all the other aspects. This requires us to interact with many people in our organizations as well as the public. When the HIPAA privacy rule was implemented versus, for instance, state privacy laws, it put the whole subject in such a limelight. In addition, when the enforcement rule came out, the penalties were so severe, it made it such that the privacy officer can't be at a level of the organization where he or she doesn't have both responsibility and authority. For example, I report to the university provost. It shows where health information management has come. We're not in the basement anymore!

Chvatal: Initially privacy officers focused exclusively on protecting patient information but the scope of our responsibilities has evolved. Now we also protect employee information and have even been pulled into discussion about our own proprietary information. We started as privacy officers for patient information and have evolved into privacy officers for any sort of information that's protected.

Fahim-Koster: It's shifted quite dramatically, partly due to the hype in the media after various incidents, particularly involving identity theft. It's raised the public's knowledge and awareness of privacy regulations and forced us to go back and say we need to protect not only personal health records but other sensitive information. Also, with advances in technology we've had to look more broadly than just HIPAA in terms of taking measures to secure data and ensure its privacy.

Gildersleeve: We have a broader role today. HIPAA's a way of life now for any covered entity, but we're still responsible for interpreting and applying HIPAA to day-to-day practices and for monitoring compliance activities. On any given day we have requests for interpretation in new areas involving the work force and corporate activities and have to look at the technical and physical safeguards we have in place to protect information.

Q: How have new privacy-related issues such as health information exchange, protection of data, compliance with state laws, and increased public interest affected the privacy officer role?

Kiel: I think one of the impacts has been our involvement in training. The privacy rule was meant to give the public greater access to their records, and it has—if the rule is followed properly. But it becomes a hindrance if people aren't trained properly. You've got to have people at the front desk with a good working knowledge of what HIPAA allows and what it doesn't. They can't be in that position and telling patients they can't have access to their charts because of HIPAA. So the privacy officer needs to be involved in training the work force to know what really is allowed and what procedures need to be followed. We also have to be available to answer questions and interpret the standards; many people look at secondary sources, such as summaries and articles on HIPAA, but our actions have to be based on the law.

Chvatal: I think we have to be more aware of initiatives at the state and federal level that have to do with personal health records and electronic health records. We have to oversee implementation and compliance with HIPAA as well as other initiatives and manage them all so that they're all in compliance with HIPAA. And we have to address the regulations with patients, who may have read a synopsis or a piece of a regulation or an article and misinterpreted what's allowed and what's not.

Fahim-Koster: My role has broadened and has an increased scope. Initially I was in my own world of HIPAA, but then there came various state laws dealing with HIV, mental health records, etc. We also have to be concerned with notification laws of other states, which we have to be aware of in the event we have patients from those states. Now I do a lot more work with risk management, corporate compliance, human resources, and the corporate counsel, and there's an intermingling of our responsibilities. You almost don't know where one person's role ends and another's begins.

Gildersleeve: It's a matter of greater interaction with the public as opposed to work force members. We get a certain number of questions regarding compliance from the work force, but we have to do more with answering the public's questions and explaining to patients what their rights are and what the process is for requesting amendments and making complaints.

Q: To what degree do you think state law privacy differences will affect successful regional health information organization implementation and health information exchange?

Kiel: When state laws and HIPAA conflict, you have to adhere to the more stringent law. Where there is some hesitation is when providers are located near adjoining states with different regulations and information would be exchanged across state lines. I think this will be addressed in the same way as telemedicine is now.

Chvatal: Between HIPAA and state laws there are a few contradictions, almost to the point where we wonder, "do we comply with HIPAA and not the state law or vice versa?" There are also inconsistencies in state law, and some counties even have regulations about how information can be shared. So state laws add an extra layer of complexity for RHIOs and make them more difficult to implement, especially when they are crossing state lines.

Fahim-Koster: A lot of those differences hinder successes from happening. Different state laws are contradictory and until there are standardized privacy and security laws across states it will be difficult to implement nationwide information exchange. It will be difficult to have the information flow freely.

Gildersleeve: State laws reinforce HIPAA and may be even more stringent. For example, 23 or 24 states have mandatory reporting if a patient's Social Security number is disclosed, but HIPAA doesn't require proactive disclosure in that circumstance. So state laws reinforce a higher standard than HIPAA. We have a modest multihospital RHIO and our approach has been conservative. We require authorization of patients to have their records included in the RHIO. Right now there's a patchwork quilt of regulations and it's a matter of national cooperation. A national standard on RHIOs would go a long way toward making them a reality.

Q: After several years of HIPAA implementation, are there standards that you feel don't work the way they were intended or lack efficacy? If so, which ones?

Kiel: An area that I'm particularly concerned about is the Family Education Rights and Privacy Act (FERPA), which deals with educational institutions. Under HIPAA the medical record is a medical record, but under FERPA, if, for example, a nurse in the college clinic writes a clinical note, it's considered an educational record. Under HIPAA, physicians and hospitals can share a patient's record for continuing care without further authorization, but under FERPA you need another authorization to treat the records as medical records. I testified about this at a hearing of the National Committee on Vital and Health Statistics and hope to see it changed.

Chvatal: Overall the intent of HIPAA was well-founded, but unfortunately the way the privacy regulations and standards were written is not cohesive. The foundation's there, but lawmakers wrote the process for an industry they weren't familiar with and the process started down the wrong path. For example, with the accounting for disclosures requirement, the intent was to give patients the right to request a list of disclosures of their information, but it only applies to a certain set of transactions. So in the four years since its was implemented, I've not had one request for an accounting of disclosures. Yet the way it was written it's cumbersome for the covered entity to comply with.

Also, there's the lack of consumer education about HIPAA. We've had people who've wanted to make a complaint because they think we violated HIPAA, but they've read part of the statute or an article with inaccurate or incomplete information. We have to explain the regulation and why we did what we did and why it wasn't in violation of HIPAA.

Fahim-Koster: The accounting for disclosures requirement. We have safeguards and processes in place to capture any inappropriate disclosures, but it's resource-intensive and time-consuming to comply with, and we're not seeing any value from it. We haven't had one request from a patient. Otherwise, in regards to security, HIPAA brought nothing new to the table from the standpoint of good security practices that any organization should have in place. However, some of the requirements are burdensome because of the complexity of healthcare. The minimum necessary has not always been an easy rule to apply over the years.

Gildersleeve: The requests for accounting of disclosures and confidential communications. We've had less than 10 of both [since those requirements went into effect] yet we have a significant infrastructure to track where the data flows and whether there have been any unauthorized disclosures. It's an unintended consequence [of the regulations] that there may be items we have no control over, that we, as a covered entity have to disclose to public health or state agencies, for instance, but they have to go into the accounting for disclosures database. And the database has a rolling six-year window in terms of a minimum requirement for retaining data, so it requires administrative resources.

On the other hand, we typically receive one or two requests for amendment each month. Sometimes these address a valid concern regarding the accuracy of the chart, for example, if the patient's birthday is incorrect. But many of the requests may involve people differing with the language of the healthcare provider, which is subjective in nature and a professional judgment of the provider. It takes time and resources to go through the amendment process.

Q: What are the greatest sources of concern for privacy officers these days?

Kiel: The example I gave of HIPAA and FERPA being inconsistent is a situation where trying to meet the law gets in the way of quality patient care and advocacy. Quality, ethical care is the number one priority, and then we should integrate the law with it.

Chvatal: HIPAA is the one rule everyone knows about, but I expect something else will come along that will change what we do and how we do it. It's keeping up with the ever-changing legislative landscape, reviewing bills, having a voice in the legislative process, then purchasing systems, and setting the privacy and security parameters so they meet the new requirements.

Fahim-Koster: What keeps me up at night is having a major security breach that will bring about a privacy breach. We put a lot of effort into our networks and applications security, but with USB devices, camera phones, and iPods with 80 [gigabyte storage capacity], someone can download your entire hard drive and carry it away in their pocket. As fast as technology is proceeding, it's exceedingly hard to keep up. It's very disconcerting.

Gildersleeve: The degree to which healthcare is dynamic. In the electronic world, things evolve rapidly, making the interpretation of HIPAA crucial. For example, the speed with which protected health information is accessible and desired by others in clinical care. A doctor wants to know test results almost in real-time. How do we do it in the electronic world in a way that's secure and HIPAA compliant?

Q: Recent surveys (including those by AHIMA) have shown a certain amount of complacency about HIPAA compliance on the part of some organizations. What are your thoughts? How are privacy officers affected by this?

Kiel: We have to be very careful in recognizing complacency and responding to it right away. Remember, the law was put in place for the patient, and it's the patient who's really the boss. We need to remember that when things are done that aren't patient friendly, like having a 16-page notice of privacy rights. What reasonable person is going to read 16 pages in order to go to the doctor?

Chvatal: I agree that there is a certain amount of complacency. Part of it is because of the enforcement model by the [US Department of Health and Human Services] Office for Civil Rights (OCR). From the beginning it said it would be the gentler, kinder enforcer, unlike [the Joint Commission] which can show up any time. OCR said that it would be complaint driven, and I think many organizations feel that if they manage the complaints they won't get an OCR review. Then, when employees see that the organization is not held to privacy regulations and there aren't consequences for lack of action, it's hard to get enthusiasm and buy-in. Recently on the security side, the Office of Inspector General (OIG) has begun some random audits. That may increase awareness a little, but the lack of enforcement when there are so many other things to comply with makes it difficult. People see that the Joint Commission, for example, is real. So far they haven't seen anything with HIPAA compliance that's real to them. That's why we incorporate it in our standard operating procedures so it's not viewed as something else [the staff] has to deal with.

Fahim-Koster: There is some complacency. When we started, a lot of organizations made resources available prior to the HIPAA implementation deadline. As it came and went without complaints and no nationwide efforts by the OCR, some executives relaxed and said, "we've done what we could do, now we need to move on." Privacy and security has to compete for resources that are perceived to be needed elsewhere. I hear OIG is starting its first security audits, and hopefully some guidance will come out of it, if OIG prepares risk assessments and a work plan based on its audits and complaints as with corporate compliance. I think that will get more attention and it will be interesting to see how the industry responds to information obtained in the audits.

Gildersleeve: I don't agree that there's complacency. The degree to which there are daily questions shows that our work force members are taking time to ask and be very compliant with the law. There's a small percentage of the public that's aware of HIPAA or who want to exercise its rights under HIPAA, but I don't believe that leads us to be complacent. Healthcare has had a sense of confidentiality from day one, so certain parts of HIPAA are not new concepts; it just formalized the process for dealing with privacy and security.

Q: Are consumers really becoming more informed regarding their health information and their rights?

Kiel: People are not becoming more informed. They hear you can get your medical record and that yes, you can amend it, but then they hit a road block because they want something that's not required by the law or the hospital or physician's office misinterprets the regulations. So we as an industry need to become more informed and be more effective in explaining to the public its rights.

Chvatal: Patients are receiving information, but it's not complete, nor is it being distributed by the correct people. Articles in consumer publications may address HIPAA but not explain the rules and/or rights correctly. Unfortunately, passage of HIPAA didn't include a means for the government to educate consumers, so they have to depend on others who might not have a complete understanding of the regulation.

Fahim-Koster: Absolutely, people are becoming more informed. Since the privacy regulations went into effect we implemented a privacy hotline for complaints and over the years there has been an increase in complaints. On the one hand that may seem alarming, but I think it shows people are more educated. It doesn't necessarily mean we have a problem. We get calls with people asking if their rights were breached, and we then explain whether they were or not. I do agree that there's a misunderstanding of the regulations, but the rule is very complex and you can't explain it quickly. Our notice of privacy practices is two pages back and front and it's so much information and there are so many nuances, unless you're in the field you might not know whether your health information privacy has been breached. I think the fact that people are asking, that they know where to call, is evidence that they're more aware. Whether they're wrong or not [in thinking their rights have been breached] is immaterial.

Gildersleeve: In our experience, when a patient complains about someone having wrongful access to their information, it's fairly concrete whether it happened or not because of audit trails. Where people are misinformed about their rights is when they want to restrict access to parts of their record and they don't realize the covered entity has the right to deny the request. Also, for most organizations, the EHR is not sufficiently granular to restrict what a patient doesn't want disclosed, or we can't guarantee that the provider they don't want to see their record won't see it again.

Q: Please comment on the perception of lack of federal "teeth" to enforce HIPAA for building privacy trust.

Kiel: The enforcement rule went into effect in March 2006, which we all must follow. When a complaint is filed with the OCR, people need to understand that the government will get to their complaint. There may be some funding issues so the response may be slow, but the complaint is put into a database and if the OCR sees a pattern, they will call back. Regardless of the speed of government response, we have patients' lives in our hands and we need to be ethical, legal, and moral in our dealings with their protected health information.

Chvatal: The lack of enforcement is not necessarily doing anything to reduce the level of trust but it's not doing anything to enforce the trust because no one's being called on the carpet. We're not seeing OCR doing random audits, and we don't hear about them levying fines. We know some complaints have been dismissed because they weren't valid and some may have been passed on to the Justice Department, but people are not seeing their complaints come to light, so that doesn't help them place trust in the system. And unfortunately right now they're hearing about bad things like breaches of systems and other lapses.

Fahim-Koster: There are more teeth now, for corporations, after passage of the Sarbanes-Oxley Act of 2002. But for HIPAA, there's been no major rah-rah in the media when patients' rights were violated. The public doesn't see the government going after people, so in the end they can't help thinking that people aren't taking it seriously.

Gildersleeve: I don't feel we need more federal teeth to enforce HIPAA. It's a complaint-driven process and that's enough to keep providers aware of their responsibilities. Take the example I gave earlier of some states requiring mandatory reporting if a patient's Social Security number is disclosed, but HIPAA not requiring it. Organizations have the choice of beefing up system security or removing the Social Security number from the system. Most feel that's too onerous so they choose to beef up security with encryption, appropriate passwords, and the like.

In a consumer-driven system, if the consumer doesn't feel he has trust in a provider, I doubt he will use the provider. That applies whether the provider uses paper or electronic records. If a complaint is received, it usually results in remediation and re-education, so if everyone takes that approach, most of the concerns will go away. By the time we got new legislation with more teeth, I don't think it would be a concern any longer because organizations would have already addressed the problem.

This is image driven also. A loss of image is far more important than going through litigation that's kept out of public view because of an out-of-court settlement. No organization wants to go before the public and say it's had a breach of healthcare information. [The industry] is so competitive it's taking more proactive steps to secure privacy.

Q: How can privacy officers influence the industry to a future in which privacy and security of health information is paramount?

Kiel: Privacy officers have to be an effective advocate and know what's going on at all levels in the organization. That means checking daily with staff to see if they've had requests to amend records or other issues or concerns. We have to be right on the ball, out there and visible in our organizations. We also need to participate in continuing education, get certified, go to conferences, talk to other people, look at best practices and learn from each other. We also need to listen to our customers and know where the issues are.

Chvatal: It's important for privacy officers to be involved and have a voice with their local, state, and federal governments when privacy and security laws are being drafted and implemented. Many of the laws, while the intent is good, are written in such a way that implementation of the law is very difficult and many times doesn't offer the protections that were intended by the law in the first place.

Fahim-Koster: We're seeing a natural movement for that to happen because of heightened public awareness. The public is saying, "Wait! My information is floating out there, and it's forcing people to take it seriously." Privacy officers are also working through organizations like AHIMA. They're good mediums to push the word out. I participate in a work group for privacy and security officers in Atlanta. It's a good way to meet, find parallels between what we're each dealing with in our own organizations, educate each other, and build momentum for changes and improvements.

Gildersleeve: By raising questions. There are certain areas of HIPAA that are still extremely gray, such as the availability of information electronically for research. [That type of data] is more easily overseen because of audit trails but as a large data warehouse it's also more accessible, and it requires us to be very scrupulous in our approach.

Report compiled by Gina Rollins.
To learn more about AHIMA, go to www.ahima.org.

In April 2007, AHIMA unveils a new version of its certification for healthcare privacy and security professionals, the Certified in Healthcare Privacy and Security (CHPS) credential. The certification will demonstrate mastery in both areas. (Previously three credentials had been offered: the Certified in Healthcare Privacy [CHP], the Certified in Healthcare Security [CHS], and the combined CHPS.)

To develop the CHPS credential, AHIMA commissioned a job analysis to obtain descriptive information about the tasks performed and knowledge needed to adequately perform those tasks. Assisting in the job analysis was a representative group of experts in healthcare privacy and security who could validate that the content covered in the examination overlapped with the important components of the job. The results of this analysis helped to develop test specifications for the CHPS certification examination. It also shed light on many of the issues discussed in this roundtable. Going forward, a committee of subject matter experts continues to work to ensure that the examination is challenging and relevant to the field. The participants in this panel have participated in either the job analysis or construction of the CHPS exam.

To learn more about the CHPS certification, go to www.ahima.org/certification.