Report on
PATIENT PRIVACY
Volume 16, Number 1 • January 2016
Practical News and Strategies for Complying With HIPAA

2016 Outlook

2016 to Bring a Sharper Focus on Threats, Training Employees, Managing Technology

By Theresa Defino, editor
tdefino@aishealth.com

HIPAA privacy and security officers and others who safeguard protected health information (PHI) don't typically ring in the new year with confidence that all nettlesome issues from the past 12 months have been resolved. They also know that new challenges lie before them — some familiar, others unimagined.

With this in mind, *RPP* queried a host of compliance officials, experts and advisors to HIPAA covered entities (CEs) and business associates (BAs) about where they plan to focus their efforts this year, whether their priorities differ from 2015 and what emerging issues they expect to tackle in 2016.

Common themes include the need to address the "Internet of Things," reduce the threats posed by workforce members through a renewed focus on training, and ensure that vital new technology doesn't inadvertently compromise PHI, among others.

The Internet of Things is the concept of myriad devices — and people — connected, wirelessly, sometimes automatically and insecurely, to the Internet. "Millions of new devices are being added to the Internet daily. Many are streaming personal data," says Rick Kam, "creating new cyber attack vectors and risk."

Kam is president and co-founder of ID Experts, a security consulting firm and provider of credit monitoring services and, more recently, a medical identity theft protection program called MIDAS *(RPP 12/15, p. 6)*. He names the new Apple Watch as one example. "The introduction of personal mobile devices to the workplace a few years ago created significant security issues. Compliance professionals will need to think about how to incorporate these new devices into the workplace and make them safe," Kam says.

David Harlow, principal with Harlow Group, LLC in Boston, agrees. "With the growth in value-based payment, there is increasing emphasis on remote monitoring and communications. Consumer grade monitors and smartphone apps need to be reviewed carefully for compliance before being put into service," he says.

The "rush" to adopt technology poses a danger, says Frank Ruelas, principal of HIPAA College and a facility compliance professional at St. Joseph's Hospital and Medical Center, which is part of Dignity Health in Phoenix, Ariz. Too often there's not enough thought given to "what compliance challenges the technology may present," Ruelas says, who points to texting as one example. "The widespread access and convenience of texting seemed to have most people automatically [assuming] that texting of information, to include protected health information, was a positive activity," he adds.

Ruelas says there's been no data to support the belief that "texting allows for a higher quality of care, better patient safety, increased levels of communication." Despite rampant texting, many institutions have yet to adopt a texting policy. "So, to me, keeping an eye on the 'application of the month' and how it may impact compliance will be a key point of focus for me in 2016," he says.

In addition, Ruelas says his "priority tasks going into 2016 include identifying how to effectively monitor and audit identified risk areas."

Knowledge of those risk areas comes from incident reports at one's own institution, Ruelas says, and also from reviewing where government agencies such as the HHS Office of Inspector General (OIG) plan to focus their efforts.

In the fiscal year 2016 OIG work plan, for instance, officials have again indicated that they plan to "determine the extent to which hospitals comply with contingency planning requirements [under HIPAA]. We will also compare hospitals' contingency plans with government- and industry-recommended practices. The HIPAA Security Rule requires covered entities to have a contingency plan that establishes policies and procedures for responding to an emergency or other occurrence that damages systems that contain protected health information."

This project has been in the OIG's Work Plan for the past two years; the newest version estimates it will be completed sometime this fiscal year.

Aside from failing to conduct a risk analysis and encryption, the neglected task that Roger Shindell, who

is founder, president and CEO of the HIPAA consulting firm of Carosh Compliance Solutions, says what he encounters the most is "inadequate training." This is evident, Shindell notes, in the corrective action plans that OCR has required of errant CEs. Nearly all of them mention inadequate training.

"The major issue is that most, if not all, organizations do training on the concepts of HIPAA," but fail to specify how the training applies to individual workers, says Shindell.

The regulations specify that CEs "must train all members of its work force on the policies and procedures with respect to PHI…as necessary and appropriate for the members of the work force to carry out their function within the covered entity," Shindell says. "In our practice we rarely find organizations that are complying with this requirement."

At Beth Israel Deaconess Medical Center (BIDMC), "user awareness training is among the 14 specific compliance areas that officials will continue to focus on this year. Others include risk management, identity management, and information security program governance, policies and procedures," John Halamka, BIDMC's chief information security officer, tells *RPP*.

BIDMC "will continue to invest millions in security technology, rewrite many of our policies and invest in continuous security education for all our staff," Halamka says on his blog at http://geekdoctor.blogspot.com. "Despite our best efforts, I cannot promise a breach-free year in 2016."

Harlow also recommends that CEs and BAs "refresh compliance training programs that may have grown stale."

"I've seen employees do the same online training and testing year after year," which means the program won't alert workers to newer threats such as phishing. "Staff must be trained — and retrained — to recognize phishing emails that get past the automated filters," Harlow says. This is particularly important because such emails are becoming increasingly more sophisticated.

Joseph Lazzarotti, a shareholder with Jackson Lewis P.C. in Morristown, N.J., takes this concept a step further: dynamic training needs to reflect dynamic policies. "In short, compliance measures and security safeguards, like technology, can quickly become obsolete and ineffective. It is critical, therefore, that covered entities continually re-evaluate their safeguards concerning privacy and security (and not just because of HIPAA), and in particular with regard to levels of access to protected health information, electronic devices used by workforce members and changes in technology," he says.

"Consider, for example, the level of turnover in a practice. If high, many newer members of the workforce may not fully appreciate the covered entity's privacy and security safeguards," Lazzarotti says. "Newer employees may not experience the same intensity that existed when the practice rolled-out its privacy and security policies. This may be the case even after newer workforce members attend training, as many covered entities have moved to more pre-packaged or online training products that tend to communicate basic principles for achieving privacy and security, not the practice's particular requirements."

Cris Ewell, chief information security officer at Seattle Children's Hospital, says his priorities for this year aren't much different from 2015, "other than digging deeper in to how to use the cloud for both PHI and FISMA related documents." FISMA, which stands for the Federal Information Security Management Act, governs security standards for government computer systems and may apply to federal data flowing through non-government computers.

"We are piloting a cloud project to see how to utilize cloud providers, such as Amazon Web Services or Microsoft, to host different types of data with different levels of implemented controls," Ewell tells *RPP*. "The data can range from general research data, PHI, and research data with a requirement for FISMA level protection. We continue to develop our risk management practices, including new algorithms to help predict areas of improvement."

In Ewell's view, the emerging issues are data sharing between health care providers, patients and researchers; increased use of mobile computing; increased external threats, including potential nation state, organized crime, hacktivists, and third parties; and medical device vulnerabilities. Ewell recently discussed his strategies for "reducing the attack surface" that may compromise PHI *(RPP 10/15, p. 1).*

Marcia Augsburger, a health care and litigation partner with King & Spalding LLP, warned about the increasing chances of criminal prosecution for improper use of PHI. In November, "a former district manager for a pharmaceutical company pleaded guilty to violating HIPAA's criminal provisions," she notes. "The district manager wrongfully accessed patients' protected PHI when he used their demographic and medical information to fill out prior authorization forms for physician signatures so that the patients could get coverage for the pharmaceutical company's drug." The physician in this case has been indicted for accepting kickbacks and has had to voluntarily surrender her license to practice.

CEs also need to be concerned that they don't run afoul of state laws. "Providers, BAs and their consultants and attorneys have put so much attention into HIPAA that they are failing to account for state law, including,

in some cases, onerous Medicaid privacy and security requirements," Augsburger says.

Kam also recommends that CEs and BAs take proactive steps this year to ensure that data aren't compromised, and to be ready if they are. "Assume you have been breached by malware and devote some amount of resources to investigate whether malware exists in your systems and those of your business associates," he says, which he calls a new task this year. "Last year, organizations tested their own critical systems. This year, organizations should expand their investigations to critical BAs."

"With the likelihood of breaches increasing each year, it is more important than ever to have an updated incident response plan that has been tested by the Incident Response Team," Kam says. This year he's also recommending that "the plan be tested by an outside expert with current threat vectors such as state sponsored hacking and malware intrusions," given how many significant security breaches happened last year.

Similarly, don't forget disaster and business continuity plans, says Rebecca Herold, an information privacy, security and compliance consultant based in Des Moines. "Update them, and test them. I've noticed many CEs and BAs are increasingly using cloud services for a wide variety of things, such as data storage, cloud-based applications, etc."

At the same time, "they are also increasingly ignoring [these plans] because they have a misguided belief that they no longer need to have such plans since they are so dependent upon cloud services," says Herold. "They assume the clouds will always make everything they need available to them. In 2016 they need to review and update their disaster recovery and business continuity plans to not only meet compliance, but also to ensure they can protect their business, and PHI, in the event of a business outage or some other type of disaster."

Kam also recommends developing "good working relationships with FBI and local law enforcement," citing the "125% increase over the past five years in criminal hacking attacks. Having the ability to reach out to law enforcement to engage them quickly if there is a criminal hacking attack will reduce the risks and costs associated with the breach response."

This approach is also favored by the FBI. In a recent interview, John Riggi, chief of the Outreach Section of the FBI's Cyber Division, described how the FBI has established cyber forces in its regional offices *(RPP 12/15, p. 1).*

Regarding breach mitigation trends, Kam says more entities are offering credit monitoring and other ID services for multiple years, recognizing that "the potential impact and risk to an individual of a data breach is increasing both in scope and cost. Now health care data are being targeted, not just financial data, and criminals are monetizing this data more effectively."

This year shouldn't be a watershed for CEs and BAs; there are no big regulations expected and no huge increase in enforcement predicted, says Jeff Drummond, a partner in the Dallas office of Jackson Walker LLP. Million-record hacks will probably continue, he adds.

"I don't think we'll see hackers get into the medical device of a high-profile politician and kill him; that will only happen in mysteries and thrillers," Drummond says. "But I do think there will be some accidental or incidental events along those lines that will get a lot of attention, and developers will start to think more about whether additional connectivity is always a good thing."

Finally, make the compliance job easier by dumping — appropriately of course — data that are no longer needed, "particularly your off-site data," says Drummond. "Figure out what your statute of limitations and state medical record retention requirements are, as well as any contractual requirements, and if you can delete data, do so," he says. "If you have the same data in multiple places, get rid of the duplicate data; you need legitimate backups, of course, but not unintentional backups. Storage is cheap, so there's a tendency for people to err on the side of keeping data longer than they need to." But, as he says, "the easiest data to protect are data you don't have."

Contact Kam at rick.kam@idexpertscorp.com, Harlow at david@harlowgroup.net, Shindell at rshindel@carosh.com, Halamka at jhalamka@bidmc.harvard.edu, Lazzarotti at lazzaroj@jacksonlewis.com, Ewell at cris.ewell@seattlechildrens.org, Augsburger at MAugsburger@KSLAW.com, Herold at rebeccaherold@rebeccaherold.com and Drummond at jdrummond@jw.com. ✧