Executive Advisory Board on Privacy & Security

Enterprise Risk Management: Successfully Achieving Privacy and Security Objectives with Third Party Relationships

April 9, 2014

eHEALTH INITIATIVE
Real Solutions. Better Health.

Introduction: Responding to a new industry regulation

The importance of securing patients' private health information is reinforced by newspaper headlines nearly every day. The names of large companies—from retailers to an ever-growing number of healthcare providers and payers—are frequently plastered across the New York Times' and Wall Street Journal's front pages, causing incalculable reputational damage to even the most trusted company names. To protect their good names, today's companies must do much more than simply guard against the catastrophic consequences of a stolen laptop or a hacker's unauthorized intrusion. Current regulations also hold companies accountable for the privacy and security safeguards implemented by their business associates.

On April 9, nineteen representatives of the payer, provider, clinical laboratory, and pharmaceutical industries came together in Washington, DC for the third meeting of the eHealth Initiative Executive Advisory Board on Privacy and Security. The chief information security officers (CISOs), chief privacy officers (CPOs), and other c-suite-level executives who make up the Advisory Board had previously met twice to articulate their top privacy and security concerns and discuss best practices to guard against breaches. During this meeting, the group concentrated on defining and minimizing the risks inherent in doing business with third-party vendors.

Many healthcare companies are discovering that their business associates have a profound lack of understanding about their privacy and security regulatory obligations. To reduce their vulnerability when doing business with third-party vendors, the panel explored ways to best protect their own interests in an increasingly interconnected environment. "The biggest challenge with third parties is that you can't monitor everything they do," said one industry representative. "So you have to do everything in your power to educate them about how to protect your data. Your reputation is on the line."

Defining the problem: What's your greatest challenge?

Upon gauging the general level of awareness within his organization of the privacy and security concerns involved when doing business with third parties, one representative of a large provider said that he was concerned by his employees' lack of knowledge. "The magnitude of all that we have to deal with regarding retaining third parties is huge," he explained. "Many in our organization do not understand privacy implications, and they don't understand how to implement technical controls to protect patient information."

The price of such ignorance can be huge. In addition to the devastating institutional fallout that the unauthorized exposure of protected health information can involve, regulators now stand at the ready to conduct privacy and security audits that can have significant monetary—and reputational—consequences to well-established payers, providers, and pharmaceutical companies.

The specter of such consequences in an age in which consumers and regulators are pushing for ever-increasing marketplace transparency can make for a perfect storm. Dan Garrett, health information technology practice leader at PwC and chair-emeritus of the eHealth Initiative board of directors, pointed out that the Centers for Medicare and Medicaid Services (CMS) had recently revealed individual physicians' Medicare payments, making front-page headlines across the country. "Transparency is a huge part of the privacy and security issue," said Garrett. "Getting data in consumer hands that can be actionable is the lifeblood of transforming this industry. But the more you do this, the greater the risk that this data will be compromised."

When asked to articulate their biggest challenges in handling privacy and security risks in relation to third parties, many of the industry representatives commented on the relative immaturity of their own and their business associates' programs to ensure the privacy and security of restricted information. "I have a large number of people who want to pick vendors without knowing the privacy and security implications," said one CISO. Another talked about the difficulty of determining who his vendors are. With the advent of the Health Information Technology for Economic and Clinical Health (HITECH) Act, his organization is retroactively identifying its business associates. "It is difficult to determine what kind of vendors we have," he explained. "Further complicating the situation is that there is a mixing of patient data among our systems and different vendor systems. If we don't know where the data came from, how can we determine who owns it?"

Rocky relationships with the physician community can also complicate an organization's adherence to privacy regulations. Despite efforts to educate doctors about how privacy and security policies are crucial to protecting patient information, several representatives said that they experience strong pushback in this area. "Doctors are used to doing their own thing," said one person. Several others agreed, adding that physician employees who come from smaller practices are often accustomed to flying "under the radar" of privacy and security regulation enforcement. Several CISOs said that presenting regulations to such physicians as efforts that can make the organization "audit-proof" may be more effective than simply giving them "government guidance" to which they must unquestioningly adhere.

Physicians' growing role in driving new technologies has made them front-line players in the continual effort to safeguard patient information. "Electronic health records (EHRs) are now ubiquitous, and physicians are not always sure who is on the receiving end of their patient data," said one CISO. Additional problems occur when physicians bring their personal mobile devices into the workplace. "This can make it nearly impossible for organizations to monitor the flow of patient information," said a representative. Others added that physicians involved in academic research can present additional problems. When payers and pharmaceutical companies share data with physician researchers, questions arise regarding who ultimately owns and is responsible for that data and how it should be transferred. The answers are often murky.

Of course, the healthcare industry is no stranger to third-party relationships. Some of these relationships go back years, even decades. And the original agreement may have stayed the same—at least on paper. “Sometimes we have been dealing with the same vendor for 20 or 30 years,” said one industry representative. “No one knows where the original agreement is; it may not even exist.” Unearthing these contracts—or drafting them from scratch—is an ambitious, but necessary, project. All agreements need to be brought up to date and in line with evolving regulatory requirements. “There should be no grey area regarding who is responsible for what,” affirmed one CISO.

Best practices: Proactively anticipating security risks

Before soliciting the industry representatives' feedback on their best practices regarding their privacy and security policies, Mick Coady, principal, Health Information Privacy and Security at PwC, asked the group about the degree to which their organizations have integrated third-party risk controls into their enterprise risk management frameworks (ERMs). When most representatives responded by saying that they have yet to fully develop their ERMs, Coady said that the industry in general lacks mature ERM programs. In this way, he explained, the financial world provides a stark contrast to the healthcare sector. "One swipe of my debit card yields all of my financial information," said Coady. "That information follows me everywhere. Mature ERMs in the healthcare sector can help us manage data like the financial industry does." Not that this will be easy, affirmed Coady. In healthcare, entities must capture and manage information over the long term. "Some legacy healthcare information is more than 50 years old," he said. "Who owns that information?"

Coady asked one CISO of a payer organization how he is currently managing his company's privacy and security risks. The person responded that because it is not feasible to audit each vendor, he must determine the best way to evaluate the general risk that business associates might pose to his organization and then further assess how to minimize that risk. The representative said his information security department uses his organization's accounts payable system to determine who is on the organization's payroll. The organization then establishes whether it is sending data to or receiving data from individual vendors. Based on that information, the information security department sends risk questionnaires to its vendors. That produces risk scores for individual business associates. The information security department then works on minimizing the risk by forwarding identified risks to management. Senior-level officials subsequently determine the organization's risk appetite—producing conversations that often end up in board-level discussions.

"Is this a perfect process?" asked the representative. "No. We need to continually ask ourselves: Have we identified the vendors that actually need to be reviewed? Which ones are they? Just the large ones? Should we include the mom and pop ones? We must continually strive to answer these questions the best we can." The representative said that one problem his organization is currently contending with is undertaking the long, slow process of reviewing and updating old contracts. He said that locating those contracts, determining if and how the contracted services have changed, and drafting new contracts that are subject to privacy and security reviews is one of the most complicated tasks the organization has undertaken.

Another provider representative expressed much of the same sentiments. "We struggle with how to establish a replicable model in which one person determines whether or not to contract with a specific third party," she explained. "We need to have basic criteria to identify who is high-risk. We don't have one group that does that." Like her payer counterpart, the provider representative said her organization uses an initial questionnaire to assess potential risks associated with introducing a new vendor into the organization. An enterprise risk committee that includes the organization's CIO evaluates those risks. The representative noted that risks are not confined to those posed by IT vendors. "Our model needs to include multiple players—legal, supply chain, privacy, researchers. They all collaborate with vendors. How do you pull all these players together? As an industry, we need to come up with a model that is scalable, understandable, and replicable—one that gets business owners to understand what is at risk and encourage third parties to respond to requests." Several other CISOs agreed that their business owners often do not participate in privacy and security efforts. "They are the ones who have relationships with the vendors," noted one person. "We need to leverage those relationships to proactively respond to any security risks."

Other topics that dominated the lively discussion included:

- **Creating a universal standard:** Expressing frustration with the multiple and evolving state and federal regulations in the healthcare sector that govern the privacy and security of sensitive data, one CISO wished aloud for a universal standard that would grant organizations certification of their privacy and security protections. “If I can be certified in some standard—any standard—for third-party attestation, and subsequently be covered regarding my third-party risks, I would gladly do that to avoid the threat of CMS audits,” affirmed the industry representative.

- **The blurring line between privacy and security:** Several CISOs agreed that their efforts to maintain the privacy and security of their data have become one and the same. “Our assessment is a joint privacy and security assessment,” said a payer representative. “When we do a third-party assessment, we hire an audit firm to do both privacy and security reviews at once. They are joined at the hip.”

- **Raising internal awareness:** Several industry representatives said they are embracing internal education as a means of raising awareness about enforcing privacy and security responsibilities among their business associates. One provider CISO said she conducts awareness trainings in the form of privacy and security “lunch and learns.” Another payer CISO said that he dedicates time to educating his business leaders about the importance of security controls and understanding the nature of the data that is being shared with vendors. A pharma CISO offered that his biggest problem is “evergreen” contracts that have not been updated for years, even decades: “I have to teach my colleagues that their contracts have to keep pace with our changing needs—whether it’s a new or established vendor.”

- **Evolving risk assessments:** One provider representative said that her organization’s initial risk assessment vendor questionnaire once consisted of 77 questions; today there are 22 questions. “We don’t necessarily need to go into all of their capabilities,” she said. “Today we are much more concerned with a vendor’s organizational culture regarding privacy and security. That tells us much more about any potential risk.” A pharma representative said that his organization makes risk questionnaires a condition of vendors’ contracts. “If they don’t do the questionnaire, they are in breach of the contract, and we can renegotiate,” he said. Another representative of the payer industry said his organization has a vendor risk matrix that ranks vendors in terms of the likelihood versus potential cost of a breach. “We then bring up that information during negotiations to ensure our concerns are addressed,” he said.

- **Moving to the cloud:** Several industry representatives agreed that moving their data to the cloud brings up a whole new set of privacy and security concerns. One provider representative said he conducts vulnerability assessments ten-fold when dealing with vendors that provide cloud-based services. “I want to make sure that our vendors are taking appropriate action so our data does not overlap with others,” the representative said. “I want to be sure they have the proper logging, auditing, and monitoring practices to keep our data safe, so I ask a lot of questions.” Other industry representatives noted that their organizations steer entirely clear of moving their data to the cloud. “I don’t think that regulations are keeping up with technology,” lamented one person, who is searching for a way to effectively vet cloud-based vendors.

Discussion with regulators: Insight into policy trends

In the second half of the day's program, industry leaders had the opportunity to talk directly to federal regulators about their specific concerns. It was a chance for them to learn more about the direction of current and upcoming efforts to promote the privacy and security of patient data. The Federal Trade Commission, The Food and Drug Administration, the Office for Civil Rights, the Office of the National Coordinator for Health Information Technology, and the National Institute of Standards and Technology were all represented at the roundtable. The government representatives launched the conversation by introducing the concerns that are currently top of mind for their agencies. Among them:

- The **Federal Trade Commission (FTC)** panelist highlighted a recent policy effort the agency has undertaken. In November 2013, the FTC held a meeting on "The Internet of Things," in which participants examined the possible repercussions of the increasing connectivity of medical devices. Although these devices hold tremendous promise to decrease costs and enhance care, consumers who use them should be educated about and consent to possible privacy and security risks. The FTC will release a report on consumer device security later this year.

- The **Food and Drug Administration (FDA)** panelist noted that while discussions regarding privacy and security five years ago referred to breaches as rare events, they are now commonplace in the industry. Such breaches affect all personal devices, and the healthcare sector can learn much from leveraging the lessons learned from other industries that are also vulnerable to compromised data. The panelist noted that even if device manufacturers do everything in their power to make their products secure, if the hospitals that use those products mishandle the data produced, patient information can be at risk.

  The panelist further reminded the group of the conclusions of the just-released Food and Drug Administration Safety and innovation Act (FDASIA) Health IT Report, in which the FDA, in cooperation with the Office of the National Coordinator for Health Information Technology and the Federal Communications Commission, presented strategies and recommendations for implementing a risk-based regulatory framework for mobile medical applications. The report recommended that products be regulated based on the relative risk they present to patient information. While higher-risk medical devices will incur more FDA oversight, lower-risk devices will have less oversight. Additionally, the FDA is pursuing stronger ties with both the Department of Homeland Security (DHS) and industry leaders to better deal with anticipated data risks in relation to evolving medical technologies.

- The panelist from the **Office for Civil Rights (OCR)** noted that the agency is emerging from a period of heavy policy implementation as required by the HITECH Act, and it is not looking to engage in any major or widespread rulemaking in the near future. OCR is currently involved in some discrete areas, but nothing as broad as an omnibus bill.

  Now that HITECH's final rules have been implemented, the OCR is consolidating its enforcement efforts. HITECH contained a number of changes to improve protections for patient information and encourage patient control and empowerment by expanding EHRs. A major part of that was bringing business associates into the realm of enforcement. The new regulations provide for penalties for business associates if they are out of compliance with privacy and security rules. Business associates are required to fully comply with the rules governing the security of electronic patient information. The OCR recognizes that this places increased liability on covered entities, and the agency has given them an additional year (until September 2014) to work through necessary contractual changes with their vendors. The next step is enforcement.

The panelist reported that the OCR is dedicated to adopting a flexible and scalable approach to its privacy and security audits. The agency recognizes that there is no such thing as absolute security and that perfection is unattainable. Rather, the OCR will focus on organizations' thought processes in relation to their security efforts. The agency will give credit to organizations that adhere as much as possible and in good faith to privacy and security regulations.

- The panelist from the **Office of the National Coordinator for Health Information Technology (ONC)** noted that in the age of health information exchanges (HIEs) and EHRs, more third parties are getting involved in the flow of healthcare information. The Affordable Care Act includes a number of provisions that depend on third parties for information transfer, further contributing to the rapid flow of "big data." When vast amounts of information from numerous sources are generated at great speed, the potential for the misappropriation of that information rises precipitously. It was also highlighted that ONC has developed new tools and resources for smaller organizations were created in cooperation with the other agencies and are now published on HealthIT.gov.

The regulators said that they recognize that there is often a lack of trust among organizations that share sensitive data. Many healthcare organizations feel that they are losing their bargaining status with their vendors. Sometimes there is nothing hindering vendors from taking healthcare organizations' sensitive information and sharing it with others in ways in which those organizations are unaware. It is often unclear who actually owns information that is commonly shared. Who controls it, and how do different players protect their interests? And since different data is sometimes subject to different regulations, how can healthcare organizations and their vendors segregate the information they handle to ensure that they are compliant with multiple state and federal privacy regulations?

Policy leaders Q&A: Current and future regulatory priorities

Asked how best to prepare for an audit, the OCR representative said that comprehensive planning can go a long way toward ensuring a smooth review process. Before undergoing an audit, the OCR asks organizations to do a self-assessment of their risks, identify possible vulnerabilities, and then develop policies, procedures, and strategies to address and remediate those risks to an acceptable level. Organizations then present that information to an OCR auditor.

The OCR representative noted that auditors do not look for any specific outcome, nor do they approach audits with predetermined actions in mind. The OCR recognizes that organizational environments are in constant flux, and regulators take that into account. The OCR representative affirmed that her office knows that there is no such thing as "perfect security," and that auditors are instead looking for signs of efforts to achieve "reasonable security."

The FDA representative agreed that his agency's audits are not "one size fits all." The range of medical devices means that the agency cannot take a monolithic approach toward security. FDA auditors look for general security preparedness in the case of a breach. Auditors want to know if companies have a response plan in place in the event of a security incident. They want to be assured that organizations will respond in a prompt, reasonable manner if their data is compromised. It is when organizations display a lack of preparation that auditors raise red flags.

The ONC representative added that organizations should approach privacy and security audits by asking themselves what information they have that others may think is valuable. Once they can pinpoint both their desirable information and their vulnerabilities, they will gain a clearer understanding of the measures they need to take to protect their information. There is an increasing trend in organized intrusions into healthcare data, and accurate anticipation of such attacks can go a long way toward proactively foiling these intrusions.

Other highlights of the regulatory panel included:

- The OCR representative stated that while the agency is not abandoning the complaint-based model, it is conceivable that the OCR's compliance perspective may lend itself more to an audit approach. For the pilot audit external auditors were used and they anticipate transitioning to internal resources for the full implementation of the program. This would mean that the agency would engage with external auditors, although such a decision has not yet been made.

- In response to an industry representative who asked if measures promoted by the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) or the Leapfrog Group will play a role in government requirements, the OCR panelist said that her group is primarily involved with external groups such as JCAHO and Leapfrog in regard to regulations that apply to business associates. The OCR is working with such groups to determine if a standardized accreditation process can apply to business associates across the board. The OCR has had some discussions with JCAHO about making some of the agency's regulations part of JCAHO's requirements.

- The FDA representative noted that the medical device community in general is behind the curve regarding cyber security. Companies are wary of sharing their security efforts with their competitors, even though doing so would help the industry as a whole with their collective cyber security efforts. The ONC representative added that the financial sector began pooling its privacy and security strategies long ago, and it has not caused the downfall of the industry.

Several industry representatives spoke about additional strategies to get the attention of business associates who may be unaware—or unconcerned—about their role in protecting sensitive patient information. “We need to hold our vendors accountable,” said Jeff Hoover, partner and US leader of Health Industries Internal Audit at PwC. “What are they responsible for? Spell it out for them.” He recommended hiring “hacker helpers” to help ensure that vendors are falling in line. “Hackers can perform attack and penetration exercises to determine where the gaps are—you’d be surprised by how many gaps exist, both at large and small vendors.”

Final thoughts

As the participants wrapped up the session, they spoke about the difficulty of convincing leaders in their organizations of the necessity of investing in privacy and security safeguards when there are so many competing priorities for funding. One provider representative noted that she is in competition with the clinical side of her business, and her organization's leadership often puts more emphasis on investing in new facilities that will attract more patients. Other representatives agreed that they need strategies to convince their leadership that investing in security is vital to their organizations' business.

Most industry representatives were forthright in admitting to the immaturity of their privacy and security programs. Peter Harries, principal and US leader of Health Information Privacy and Security at PwC, said a solid risk assessment strategy is a crucial starting point to implementing such a program. "Without comprehensive risk assessment, there is only a random collection of efforts," said Harries. "You need a systemic way of ensuring ongoing compliance with your efforts."

The OCR panelist agreed, saying that solid risk-assessment strategies are essential building blocks to achieving smooth audits. To be successful, these strategies should take into account and be consistent with an organization's existing culture as it relates to privacy and security. No two security programs are going to look the same, the policy leaders emphasized. Businesses need to determine where their weaknesses are and integrate their remediation efforts within existing privacy policies. If the policies are not there, create them so that they reflect the organization's brand and priorities.

One payer representative said he represents himself to his leadership as the protector of his organization's brand. He conveys to his company's hierarchy that having their company end up in the papers due to a breach can do incalculable damage to their bottom line. Harries agreed, saying, "Linking brand protection to patient safety and revenue can go a long way toward associating privacy and security to the bottom line and getting the attention of a company's leadership."

eHI Executive Advisory Board on Privacy & Security Acknowledgments

Agatha O’Malley, Privacy Officer, Shire

Allison Viola, Vice President, Policy and Government Affairs, eHealth Initiative

Anahi Santiago, Information Security and Privacy Officer, Albert Einstein Health Network

Anne Adams, Chief Compliance Officer; Chief Privacy Officer, Emory University

Barbara Gabriel, Lead Editor, Healthcare, PwC

Bill Cushing, Division CIO/CTO, Blue Cross and Blue Shield of Massachusetts, Inc.

Cathy Beech, Chief information Security Officer, The Children’s Hospital of Philadelphia

Cora Han, Attorney, Division of Privacy & Identity Protection, Federal Trade Commission

Daniel Garrett, Principal and US Health Information Technology Leader, PwC

Dave Snyder, Chief Information Security Leader, Director of Information Security and Risk Management, Independence Blue Cross

Hussein Syed, Director, IT Security, Barnabas Health Care System

Jeff Hoover, Partner, Health Industries Internal Audit Leader, PwC

Jena Lee, Senior Vice President, Corp Compliance and Information Security, CareCore National, LLC

Jennifer Covich Bordenick, Chief Executive Officer, eHealth Initiative

Joseph Johnson, Chief Information Security Officer, CHS Health Services

Joy Pritts, Chief Privacy Officer, Office of the National Coordinator for Health Information Technology

Keith Henkell, Information Security Officer (ISO), CenterLight Health System

Kenia Rincon, Manager, Health Information Privacy and Security Practice, PwC

Kevin Stein, Information Security Specialist, Computer Security Division, Security Management and Assurance Group, National Institute for Standards and Technology

Kim Fleurquin, Chief Risk Officer, Sonora Quest Laboratories/Laboratory Sciences of Arizona

Mark Lantzy, Independent Consultant

Mark Savage, Director of Health IT Policy and Programs, National Partnership for Women & Families

Mick Coady, Principal, Health Information Privacy and Security Practice, PwC

Mitch Parker, Chief Information Security Officer, Temple University Health System, Inc.

Nadia Leather, Director, Health Industries Marketing, PwC

Paul Shenenberger, CIO & Security Officer, Summit Medical Group

Peter Harries, Principal and US Health Information Privacy and Security Leader, Healthcare, PwC

Ralph Lange, Director, Enterprise Infrastructure, Availity

Randy Prueitt, Divisional Vice President, Global IS Business Operations Quality and Regulatory Abbott Laboratories

Ronald Mehring, Director, Information Security, Texas Health Resources

Sara A. Juster, Associate General Counsel & Privacy Officer, Surescripts

Susan McAndrews, Deputy Director, Health Information Privacy, Office for Civil Rights

William Maisel, MD, Deputy Center Director for Science, CDRH & Chief Scientist, Food and Drug Administration