Executive Advisory Board On Privacy And Security

New Care Delivery Models and Patient Control of their Data

March 3, 2015

eHEALTH INITIATIVE
Real Solutions. Better Health.

Introduction

On March 3, 2015, the eHealth Initiative (eHI) Executive Advisory Board on Privacy and Security met for the fifth time in Washington, DC. Motivated by their mutual goal to protect sensitive patient information, the chief information security officers, chief privacy officers, and other c-suite executives who make up the board wanted to take the opportunity to engage more deeply with the federal regulatory agencies that oversee the protection of private health information. To that end, representatives from the Federal Trade Commission (FTC); the US Department of Health and Human Services' (HHS) Office of Civil Rights (OCR); the Office of the National Coordinator for Health Information Technology (ONC); and the Office of Emergency Preparedness/Operations and Medical Countermeasures in the Center for Devices and Radiological Health in the Food and Drug Administration (FDA) also attended the meeting.

The gathering consisted of a lively exchange among the industry participants and regulatory representatives, during which regulators solicited and fielded questions about evolving risks to patient information and countermeasures to those risks. Specifically, the group addressed new healthcare delivery models (mobile technology in particular) and how those models are affecting patient and provider access to personal health information.

Setting The Agenda

At the start of the meeting, the participants were invited to introduce themselves and share their organizations' greatest challenges regarding preserving the safety and security of patient health information.

Several participants said that educating their organizations' boards and c-suites about the importance of adequately investing in protecting their patient data continues to be a significant challenge. While some participants said that it is difficult for them to get their boards to prioritize security concerns, others said that their boards proactively ask for information on privacy and security; the challenge is being able to educate them sufficiently enough so they can make informed decisions. Several participants brought up the difficulties presented when c-suite members get distracted by "the latest shiny object" in digital technology without considering the privacy and security risks that new technologies may pose to their organizations.

Another common concern is the ongoing anxiety over the handling of patient data passed on to third-party vendors, or business associates. Getting vendors to sufficiently understand their privacy and security responsibilities, said one participant, has thus far proved elusive. Other participants cited the ongoing need for privacy and security staff and the shortage of talent in this space; the difficultly of meeting the inconsistent regulations issued by state, federal, and local governments; and the need to educate employees about phishing scams that can open the door to data hacks. One participant noted that he often feels like the technology on which his organization depends is evolving faster than security experts can control it. Another simply stated that his main goal is to keep his organization "out of the newspapers."

Barriers to Technology Adoption

Joe Greene, a partner at PricewaterhouseCoopers (PwC), presented the chief findings of a recent PwC Healthcare Research Institute study on innovations in healthcare delivery. The study, in which 1,000 care providers were surveyed and 25 industry executives were interviewed, found that industry leaders across health plans, hospitals, and the pharmaceutical industry all perceive major shifts occurring in how care is being delivered. The majority expressed their expectation that digital technology will bridge the time, distance, and expectation gaps that currently place communication barriers between patients and their physicians.

The survey asked participants about where technology is affecting healthcare delivery and how patients and physicians are accessing that technology. PwC found that privacy concerns and a lack of financial incentives to deliver healthcare via new technologies are the chief barriers to provider adoption of mobile health. But at the same time, physicians report performing significantly more of their duties on a mobile device. Whereas in 2010, only 12% of respondents reported using mobile devices to access medical records, in 2014, 45% reported doing so. And both consumers and physicians are receptive to using mobile devices to conduct "do it yourself" healthcare, such as diagnosing strep throat and ear infections at home.

Board member participants discussed the barriers to using mobile technology in healthcare delivery that they perceive. One said that he sees physicians hesitant to use texting to communicate in the workplace in the absence of clear regulatory policy governing the use of texts to transfer patient information. Another participant said that she sees physicians intimidated by complex log-in procedures and the security measures that surround their work. "They feel like 'Big Brother' is watching," she said. As a result, physicians are now as concerned about their own privacy as they are about the security of their patients' information. Someone else added that she is seeing physicians shy away from using new technologies as a result, and that some physicians even use this fear as an excuse not to adopt unfamiliar technologies. However, it was also noted that not all physicians feel this way. In particular, medical students entering the profession are expecting to use new technologies in their jobs, and many are demanding access to it.

Data-Sharing Obstacles

With the inevitable march toward the continual adoption of new ways to communicate via mobile technology, many questions remain. "How do we get this mobile information into our medical records?" asked one participant. "Right now, we can't do that. And which devices are we going to support? Different devices require different technologies. Data-sharing is a huge problem among devices and organizations using different technologies."

When participants discussed how physicians will be reimbursed for care delivered via mobile technology, one board member said that her organization has a billing code for "virtual treatment." "The technology also allows us to utilize mid-level providers to diagnose long-distance—something we don't need doctors for," she said. "This lowers cost."

"If we are moving into a pay-for-quality world, all of this should be coming together," agreed another participant, "since this type of healthcare delivery costs much less." However, several people noted that continually obtaining patient consent for different types of information collection creates undue barriers to this type of care delivery.

Finally, a participant summed up the conversation by saying that the profession needs a security strategy that spans multiple delivery models. "We need to address how we provide security on a tactical level," he said. "Regardless of the type of device, we need the same strategic pillars to secure data. We need same strategies regardless of use case. We need front-end use case design, rather than back-end.".

Conversation With Regulators: Prioritizing Concerns

Participants were given the opportunity to discuss their chief concerns about mobile technology with the regulatory representatives present. But before addressing those concerns, the representatives articulated what they perceive as the chief privacy and security issues regarding new models of healthcare delivery and the new technologies being used to provide care. One representative remarked that many consumers erroneously assume that all of their information is protected in the same way, while the truth is that not all regulations fall under the same agency, and regulations can vary based on the type of device or application used. This puts the industry in the position of sorting out their different responsibilities to protect patient data in all of its forms as more and more sensitive information is generated and passed among patients, providers, payers, and pharma.

One regulatory representative addressed the suitability of the 15-year-old Health Insurance Portability and Accountability Act (HIPAA) to adequately govern the protection of patient information today. She said that HIPAA regulations provide flexibility for different models of care. More important than whether specific technologies are HIPAA-compliant, said the representative, is whether providers continually examine how patient information may be used, who is using it, and how to protect it.

Questions and Answer: The Quest For Compliance

In response to the regulatory representatives' invitation to the group to ask questions about the barriers they see to protecting patient health information, participants asked the representatives to respond to a number of concerns. One chief concern was liability limits. With recent security breach headlines fresh in their minds, the group was particularly interested in having the regulators address this topic. They expressed their desire for a prescriptive approach from federal regulators detailing how they can protect themselves in the event of a data breach. "How can we ensure we are doing everything we can, given that it is still not enough?" asked one participant.

The representatives responded that they have not set specific privacy and security regulations because since technology is changing so quickly, those safeguards would be outdated before they could be fully implemented. One representative advised participants to enforce a series of best practices, including conducting a thorough analysis of their risks, implementing documented safeguards, regularly updating privacy and security plans, and conducting ongoing training for employees. An ongoing, active consideration of risk management is of most importance to regulators, she said.

Several participants expressed the need for immunity from prosecution in the event of a breach. The threat of such prosecution, they said, prevents companies that have been hacked from sharing valuable information that, in the wake of a breach, could benefit everyone. PwC's Joe Greene noted that when a large breach occurs, the targeted

organization is first treated as a victim that is actively aided by law enforcement to gauge the extent of the damage and notify affected parties. However, it is not long before that same organization is treated as a defendant, held accountable for everything that happened both before and after the breach. "I don't think there will ever be immunity, but there needs to be some protections to encourage information-sharing," said Greene.

Another concern, which has been repeatedly brought up in past eHI advisory board meetings, is the responsibility of healthcare organizations to ensure that their business associates are HIPAA-compliant. "I feel hampered, held hostage to get vendors to implement safeguards, to provide system updates, or certify that updates can be put into the system," said one participant. "And I'm not talking just about the little guys—this is also a problem with large companies. Are there any resources for healthcare organizations to get these vendors to fulfill their security requirements?"

One regulatory representative responded that while HIPAA does not provide organizations with such tools, it is advisable to document any security shortcomings among business vendors and then file a complaint with regulators. However, she acknowledged that there is a significant backlog of such complaints—totaling more than 10,000. But she added that if multiple organizations express concerns about the same vendor, such concerns would likely receive attention faster.

The regulatory representatives wrapped up the session by stating that they have plans to roll out a proactive audit program of privacy and security measures in the near future in the hopes of foiling potential breaches before they occur. Without giving specific details, they noted that there will be two types of audits: one very targeted audit of specific rules, and one broad-based, on-site audit program.

The Conversation Continues: Governmental Efforts To Help An Industry Help Itself

During the second half of the meeting, the advisory board was joined by two additional regulatory representatives who attempted to shine more light on the direction of government oversight of the transmission of healthcare information. According to one representative, the role of regulatory agencies is to help organizations determine what constitutes a "real" security problem. She affirmed that federal regulators are working hard to clarify privacy and security regulations and help healthcare organizations understand and access them. She acknowledged that federal agencies are often asked to provide a prescriptive list of "to-do" items that organizations can check off to ensure they are compliant. Unfortunately, she said, it's not that easy, since as soon as such a list would be published, the "bad guys" would most likely find a way around it. However, the representative said, the industry should not forget the fact that organizations that have implemented reasonable privacy and security protections succeed in thwarting breaches of sensitive information each day. It is only the handful of successful attacks that make the front pages.

Another representative gave an update on a recent workshop sponsored by the FDA about changes to pre-market medical device submissions. The FDA is now examining how manufacturers are incorporating cybersecurity measures into the development of medical devices. Regarding devices that are already on the market, the agency is also developing post-market management of the devices' security. The FDA hopes to issue guidance on post-market surveillance by September 2015.

The regulatory representatives acknowledged the difficulty of securing medical devices, and they said that they must triage these concerns to prioritize which problems should be addressed by regulatory agencies and which should be remediated by the healthcare community. In the end, relatively few issues will rise to the level of FDA action, they said; most will need to be addressed by manufacturers. The representatives also said that the healthcare community as a whole will need to create a system by which that can happen—manufacturers should not have to address this entirely on their own. Any finger-pointing among providers and device manufacturers will have to end to effectively address device security.

One representative mentioned an upcoming Homeland Security exercise with an emphasis on the healthcare sector that will take place in 2016. She stated that the federal government wants to involve providers and medical and electronic device manufacturers from the private sector in the exercise. Helping plan, develop, and participate in the exercise, she said, is a prime opportunity to be involved in setting expectations for privacy and security.

Finally, in response to the problem of monitoring healthcare data when it leaves the traditional medical environment, one representative noted that the federal government recently took testimony on the gaps in big data from a consumer perspective. She said that with $4 billion in venture capital going into mobile apps, many business models depend on the existence of regulations to protect consumer data. The federal government is working with the mobile health industry to continue to secure and safeguard the data produced by the use of the exploding number of apps, and it encourages all industry players to work with them.

Final Thoughts: Looking Ahead

At the close of the meeting, participants shared their ongoing concerns regarding the privacy and security of emerging technologies and what topics they'd like to see addressed in future meetings of the Executive Advisory Board on Privacy and Security. The topics suggested included the protection of self-generated patient data; identity and access management in the context of medical devices; third-party certification and security; the vulnerability of patient data to international "bad actors"; and the danger posed by healthcare organizations' possession of vast volumes of patient Social Security numbers.

One participant suggested that future meetings address not only privacy and security from a regulatory perspective, but also from a legislative perspective. "What legislation on the horizon will affect us?" he asked. Another participant said that the group has the potential to collaboratively develop strategies to educate their CEOs and boards of directors on the

importance of adequately addressing and funding privacy and security safeguards. Other suggested topics included examining the use of data beyond privacy concerns, especially the way in which the next generation perceives it. "The younger generation does not think about privacy the way older generations do," said one participant. "What will privacy look like in the future, beyond the HIPAA perspective?"

The concerns expressed at the meeting were best summed up by a participant who shared a story about her daughter, who broke her wrist during a family ski vacation. Because the daughter was outside of her home state when the accident occurred, over the course of her diagnosis, treatment, and rehab, she received treatment from providers in three different states, none of which were equipped to communicate patient information to one another. As a result, the daughter underwent a significant duplication of costly tests that incurred unnecessary expense, and her medical and identification information is now hosted on several provider systems across multiple states.

In the words of one participant, "We can do better than that."

eHealth Initiative Executive Advisory Board on Privacy and Security

Acknowledgments

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

Andy Woods, Director, Regulatory Compliance and Risk, Availity

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

Brian DuPerre, Vice-president and Deputy General Counsel & Chief Privacy Officer, UnitedHealthcare

Cathy Beech, Chief Information Security Officer, Children's Hospital of Philadelphia

Christopher Kido, Managing Director, Cybersecurity and Privacy, Health Industries, PwC
Christopher Santucchi, Director, PwC

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

Dustin Wilcox, Chief Information Security Officer, Centene

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

Jay Cline, Principal, Assurance Services, PwC

Jason Newman, Chief Information Security Officer, Blue Cross Blue Shield of Minnesota

Jennifer Covich-Bordenick, Chief Executive Officer, eHealth Initiative

Jeremy Diebling, Director, Cybersecurity and Privacy, Health Industries, PwC

Joseph Greene, Principal, Cybersecurity and Privacy, Health Industries, PwC

Joseph Johnson, Chief Information Security Officer, Premise Health

Kate Gallagher, Senior Policy Analyst, America's Health Insurance Plans

Kathy Jobes, Chief Information Security Officer, Sentara

Keith Henkell, Information Security Officer, CenterLight Health System

Kenia Rincón, Director, Cybersecurity and Privacy, Health Industries, PwC

Mark Lantzy, Chief Information Officer, Gateway Health Plan

Mike Close, Vice-president Information Technology, Perkin Elmer

Mike Matteo, Chief Information Security Officer, CenterLight Health System

Nalneesh Gaur, Director, Healthcare, PwC

Neal Baker, Vice-president and Chief Privacy Officer, CVS

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

Ralph Lange, Director, Enterprise Infrastructure, Availity

Randy Prueitt, Divisional Vice-president, Global IS Business Operation Quality and Regulatory, Abbot Laboratories

Sara Juster, Associate General Counsel & Privacy Officer, Surescripts

Terence Rice, Assistant Vice-president, Risk Management and Security; Chief Information Security Officer, Merck

Tim Alcorn, Director of Technology Applications and Privacy, Janssen Diagnostics

Tracy Okubo, Senior Director, Health IT Stakeholder Outreach, eHealth Initiative