Executive Advisory Board on Privacy and Security Meeting

Shifting Foundations in the Healthcare Cybersecurity Regulatory Environment

March 30, 2016

The eHealth Initiative (eHI) Executive Advisory Board on Privacy and Security met on March 30, 2016 in Washington, DC, to explore strategies and regulations for protecting sensitive patient health information. As in previous meetings, participants included c-suite officers as well as government regulatory representatives responsible for helping secure such information. The regulatory participants represented the Food and Drug Administration (FDA), the Office for Civil Rights (OCR), the Office of the National Coordinator (ONC), and the Federal Trade Commission (FTC).

In his welcome message to the assembled group of 41, Dan Garrett, Principle at PwC, reminded everyone in the room of their interdependence, saying it matters not what new frontiers their individual companies pursue in the field of information technology if access to that information is not essentially trusted by its users. “We cannot progress without solving basic privacy issues,” said Garrett. “The more you digitally connect with your patients, the more cyber risk there is. Our responsibility is to address this issue and move the industry forward. We can’t go alone; you can’t do it within the confines of your organization. We can only do this by working together.”

When asked to identify the chief privacy and security challenges facing their organizations, advisory board participants gave voice to a variety of sentiments. One individual said that while he recognizes that a silver bullet is unlikely, solutions that enable safe information sharing are within reach. Others spoke of challenges related to organizational boards of directors and their interest in cybersecurity without really understanding it. Some individuals spoke of the challenges related to advancing capabilities in population health—a goal fraught with privacy minefields.

“How do you leverage data, be innovative, and at the same time adhere to local compliance programs?” asked one participant. “How do you work before and after with law enforcement? Enforcement can help but is also our regulator.” Another dominant theme among participants was the vital necessity of gaining the trust of consumers in a world in which security compromises are everyday news. “We need to be sensitive to what patients want to share and what they do not want to share,” said one participant. “How do we educate patients and members without scaring them? If no one shares, no one benefits.”

Participants expressed that progress will require transparency, collaboration, and national coordination among providers, payers, pharma, and other stakeholder groups. Although ideal in theory, to achieve this multi-sectoral counter-response to the privacy issues that we are facing as an industry, we must first identify and uproot the barriers that have been lodged within the system. One of the identified barriers is the siloed nature of the industry, which is driven by competitive forces that hinder the willingness to share data. This inherent idiosyncrasy is incompatible with national data-sharing goals and may require a cultural shift and strategic realignment within organizations. Federal regulations have attempted to push providers toward

interoperable sharing of information, but there is need for internal change to invest in collaborative initiatives with other providers.

Freedom to share

To address the primary challenge of balancing the need for greater patient data sharing with warding off threats to that data's security, on December 18, 2015, President Obama signed into law the Cybersecurity Information Sharing Act (CISA), designed to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats." The House Committee on Rules described the measure as "a voluntary cybersecurity information-sharing process that will encourage public and private sector entities to share cyber threat information, without legal barriers and the threat of unfounded litigation—while protecting private information."

The bill's section 405 deals specifically with cybersecurity threats as they relate to healthcare. It is an answer to the government's observation that fear of punitive action keeps companies from sharing information with the government in the event of a breach. The value of the new sharing system that CISA creates is that it relieves organizations from worrying about retribution under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) when it comes to sharing cybersecurity data, because companies that come forth with cybersecurity concerns will be protected. Section 405 is expected to have a collaborative effect. The more entities come forward to share information about vulnerabilities and hacking incidents, the stronger each entity that has access to that information will become. This collective knowledge will fortify everyone's efforts to fend off cybercrime in its many forms. For its part, the government will declassify some information and share information previously unreleased. By giving companies liability protection under this bill for sharing information, the government is sending a clear signal that companies should no longer be punished for cybercrimes perpetrated against them.

What was not addressed in the discussion was how the government intends to actually incentivize providers to participate in this voluntary data sharing. Participants recognized that if covered entities do not see the immediate and tangible benefits of disclosing their data to the government, it is likely that they will elect to observe without participating until this new system has been tried and proven.

HIPAA Office of Civil Rights (OCR) Phase 2 Audit Outlook

The HHS Office for Civil Rights launched has launched Phase 2 of its HIPAA Audit Program, which will apply to both covered entities and their business associates. According to HHS's web site, "OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted."[1]

[1] "OCR Launches Phase 2 of HIPAA Audit Program," HHS.gov, Health Information Privacy. (http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html)

According to the OCR representative present, Phase 1 of the audits, conducted last year, resulted in six monetary settlements, one upheld by a judge for $10 million. Nevertheless, the imposition of civil monetary penalties remains rare. The overwhelming preference is to settle any issues through voluntary corrective action or settlements. During Phase I, said the representative, many entities were found not to be fulfilling basic security requirements—those fined generally involved stolen unencrypted laptops.

In Phase 2, the OCR will select 200 entities for desk audits and a smaller number for full, on-site audits. The initial batch of emails sent to selected entities has already gone out. Once these are replied to, entities will be asked to complete a questionnaire. The completed questionnaires will form a pool from which the organizations to be audited will be selected.

Starting in May, desk audits will begin for the selected organizations, which will be given 30 days to comply with audit requests. A smaller number of organizations will be selected for full, on-site audits. Audited entities will be asked to supply a list of business associates to which the OCR will send questionnaires. At the conclusion of the audit, each organization will receive a report and be given an opportunity to respond. OCR expects to have the audits completed by the end of the calendar year. The OCR representative emphasized that the audits were primarily being used as an educational experience rather than for punitive purposes.

Safe Harbor v. Privacy Shield

Privacy Shield is a new framework that will govern the flow of personal information between the EU and the US. It replaces the Safe Harbor framework, which was struck down by the European Court of Justice on the grounds that it violated European privacy rights. Privacy Shield puts into place mechanisms to ensure that the personal information of EU citizens is protected according to EU standards when it is sent to the US. As such, it contains provisions that require US companies wishing to import personal data from the EU to commit to "robust obligations" to protect that data. According to the European Commission:

"*The new arrangement will provide stronger obligations on companies in the US to protect the personal data of Europeans and stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities. The new arrangement includes commitments by the US that possibilities under US law for public authorities to access personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, preventing generalised access. Europeans will have the possibility to raise any enquiry or complaint in this context with a dedicated new Ombudsperson.*"[2]

Privacy Shield introduces substantial changes for data protection, including more rights for EU citizens, stricter compliance requirements for US organizations, and new limitations on government access to personal data. Additionally, it will enable an easier referral process and better cooperation between the Federal Trade Commission (FTC) and the Data Protection Authorities (DPAs). According to the FTC representative, enforcement of Safe Harbor was rare, with the FTC bringing 36 cases in 15 years. He noted that he expects the enforcement of

[2] "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield," European Commission press release, February 2, 2016. (http://europa.eu/rapid/press-release_IP-16-216_en.htm)

Privacy Shield to be very different, especially since the EU will have more direct enforcement rights.

Medical Device Cybersecurity

A representative from the FDA addressed cybersecurity risk management in the context of the FDA's proposed guidance, "Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff." The representative said that the guidance is, in part, a response to the fact that 50% of pre-market submissions for medical devices do not address cybersecurity.

The threat of cyberattacks against medical devices is a real danger to the health of patients and the integrity of the medical profession. With the increased occurrence of ransomware attacks, participants stressed the need for vendors to work closely with the FDA to identify possible access points and predict the potential of future breaches.

The representative explained that the FDA's approach is to encourage manufacturers to find and fix defects rather than to intimidate and prosecute them. The FDA acknowledges that some defects may not be due to negligence and would like manufacturers to work with them to improve the safety of devices and to safeguard against potential hacking.

The FDA representative highlighted that although the guidance is not mandatory, medical device manufacturers and hospital providers should begin to incorporate considerations for future-looking regulations and requirements in the Medical Device Pre-Market approval process. The guidance addresses the creation of a framework for assessing the security and clinical risk of marketed devices using current regulation. According to the draft guidance:

"For the majority of cases, actions taken by manufacturers to address cybersecurity vulnerabilities and exploits are considered 'cybersecurity routine updates or patches,' for which the FDA does not require advance notification or reporting under 21 CFR part 806. For a small subset of cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death, the FDA would require medical device manufacturers to notify the Agency."[3]

The guidance goes on to state that manufacturers should "establish, document, and maintain" throughout the lifecycle of a medical device a process for identifying hazards associated with the cybersecurity of the device, "estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls."

The representative emphasized that what the FDA is trying to do is essentially target risks at the overlap of security risks and clinical risks—what he referred to as "essential clinical performance" (ECP). He admitted that the industry is just coming to terms with this challenge. "It's all about taking baby steps to get people to start to think about cybersecurity with medical devices," he said.

[3] "Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff," U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Office of the Center Director, January 22, 2016. (http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf)

Key takeaways

The final discussion revealed the confounding issues that must first be unraveled before we are able to collectively defend ourselves against cyberattacks. Participants voiced that defining relationships and expectations among stakeholders is critical to ensuring the convergence of efforts to find a solution. Patients need to understand how they can guard their data, the signs that an unauthorized party has accessed their data, and the steps to take to notify their provider and insurance company should a breach occur. Providers need to clearly understand what security infrastructure is required from a regulatory stand point, the reporting procedure in the case of a breach and how to use data to identify access points that can be targeted by perpetrators. Regulators need to clearly communicate and standardize the technical requirements for security infrastructure, the reporting guidelines for suspicious activity or breaches, and the data sharing expectations and procedures for covered entities.

There was much excitement about the information presented at the meeting, and even more about the new questions that information had opened up. As each participant shared his or her key takeaways from the session, several distinct themes emerged:

- **We need to be proactive rather than reactive.** We are getting better at being retrospective (sharing information after we have been hacked), but not much better at being proactive. We need to establish the *why* of cybersecurity (why organizations are so vulnerable to attack) before we are forced into the *what* and the *how* after an attack. This is what should guide future policies.
- **We should look to other industries for guidance.** Why is the financial services industry so much better at warding off attacks? We need to evaluate the effective measures that industries outside of healthcare are taking.
- **We should partner with patients.** A lot of the time we only detect medical theft when educated consumers come to us with information. How do we better partner with patients in the fight against medical identity theft?
- **We should explore issues on a global stage.** Information-sharing has increased, but it is still very much based in the US. Joint information sharing from a global perspective would allow us to better confront issues like cybersecurity that cross national boundaries.

One participant summed up the conversation with a fitting analogy: “The scale of our organization and our goal of protecting patient information is like navigating an aircraft carrier through a series of hairpin turns. It’s difficult—but not impossible.”

March 30 Attendees

Josh Alexander, Professional Staff Member and Minority Counsel, U.S. Senate Select Committee on Intelligence

Trish Alexander, Research Director, Klas Research

Carl Anderson, Vice President, Van Scoyoc Associates

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

Seth Carmody, PhD, Device Reviewer, Director of Center for Devices and Radiological Health, Food and Drug Administration, HHS

William Cushing, Senior Vice President and Chief Audit Executive, Blue Cross and Blue Shield of Massachusetts, Inc.

Edward Ferrara, CISO, CSL Behring

Brian Files, Director, Public Policy, CVSHealth

Kendyl Hall, Cybersecurity, Architecture, Risk & Engineering (CARE), Amgen, Inc.

Keith Henkell, Information Security Officer, CenterLight Health System

Brian Ivie, CISO, BILL & MELINDA GATES FOUNDATION

Joseph ("Joey") Johnson, Chief Information Security Officer, Premise Health

Sara Juster, Associate General Counsel & Privacy Officer, Surescripts

Thien Lam, Director, IS Security and Information Security Officer, BayCare Health System

Ralph Lange, Director, Enterprise Infrastructure, Availity

Andrea Leeb, Chief Privacy Officer, Cal INDEX

Aaron Lewter, CISSP, GCIH, Director of Information Security, Head of Network & Security Services, Availity

Maurice Andrew Malcolm, Information Systems Program Manager, University of Maryland Medical System

Amber Manko, Director, Federal Affairs, America's Health Insurance Plans "AHIP"

Doug Mayer, Information Security Officer, Otsuka Pharmaceutical Development & Commercialization, Inc

Deven McGraw, Deputy Director for Health Information Privacy, Office for Civil Rights, HHS

Kevin Moriarty, Division of Privacy & Identify Protection, Federal Trade Commission

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

Eric Pickney, CISO, Sonora Quest Laboratories/Laboratory Sciences of Arizona

Michael Rushinsky, Director, Information Security & Compliance, Information Services, Indiana University Health

Anahi Santiago, Chief Information Security Officer, Christiana Care Health System

Lucia Savage, Chief Privacy Officer, Office of the National Coordinator, HHS

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

Boyd Steward, Research Director, Klas Research

Chad Thiemann, Privacy Corrector, CVS

Ted Webster, VP, Chief Security and Privacy Office, Healthplans, Inc.

Marcy Wilder, Director, Privacy and information Management practice group, Hogan Lovells

Edward You, Supervisory Special Agent, Weapons of Mass Destruction Directorate, FBI