Executive Advisory Board on Privacy and Security Meeting
Balancing Between Data Access and Risk

November 5, 2015

Introduction

The eHealth Initiative (eHI) Executive Advisory Board on Privacy and Security met on November 5, 2015 in Washington, DC, to explore strategies for balancing the increasing need for access to patient data with the necessity of safeguarding sensitive patient information. As in previous meetings, participants included c-suite officers from provider, payer, and biotechnology organizations, as well as several federal representatives from agencies responsible for helping the industry secure sensitive information. Federal agencies represented at the meeting included the Department of Health and Human Services (HHS), the HHS Office for Civil Rights (OCR), the HHS Office of the National Coordinator for Health IT (ONC), the Federal Trade Commission (FTC), and the White House Office of Science and Technology Policy (OSTP).

Although privacy and security officers at healthcare organizations may reflexively think to restrict access to protect sensitive patient data, keeping that data behind firewalls, credentialing users, and deploying complex user agreements can also have the unintended effect of stifling innovation, preventing care coordination, and driving up costs. While strong security measures are essential components of any healthcare cybersecurity plan, they should coexist with policies that enable secure data sharing that can ultimately prove beneficial to patient care.

Of course, crafting a cybersecurity approach that enables more open access to data while still protecting patient confidentiality and maintaining security is challenging. When opening the meeting, eHealth Initiative's CEO, Jennifer Covich Bordenick, reminded the group that, given the data needs of effective population health management and value-based care, it is more important than ever that healthcare organizations effectively promote data exchange. "We have talked a lot about the risks of sharing data," said Covich Bordenick, "but at the same time, we want to be able to take advantage of all of the data we generate. We must remember that data is not knowledge. We need to be able to take it and manipulate it to *create* knowledge. We want to explore how to do that safely today."

Dan Garrett, a Principle in the Healthcare Cybersecurity and Privacy practice at PwC, noted that data analytics are increasingly driving healthcare operations and asked attendees to consider how their organizations are using analytics today and in the future: "How will analytics affect how you take your drugs to market?" asked Garrett. "How are you using them to enhance patient care delivery? How can they help you handle claims? If we lock down data and throw away the key, all of that potential will be lost."

Throughout the meeting, participants were asked to address the following questions:

- What value can healthcare organizations recognize by facilitating more widespread data sharing?
- How can data sharing improve clinical or operational efficiency?
- How can organizations strike an appropriate balance between securing data and enabling use?
- What collaborative efforts are organizations undertaking to improve data sharing, and what lessons can we learn from them?

Garrett and Covich Bordenick noted that by digitizing healthcare data, organizations have created powerful new datasets that stakeholders can access and analyze to drive improvements in care delivery and business operations. Instead of individual sets of paper records spread across disparate settings, many organizations now have centralized repositories of healthcare data.

Centralizing data collection can help organizations take a more comprehensive view of their patient population, but these repositories are also tempting targets for intrusions, breaches, or other forms of cyberattack. As such, preparing for and responding to cyberattacks is a critical piece of any data management strategy. Privacy and security officers that recognize the importance of increasing access to data need to carefully consider how they will respond if their organization's data repositories are compromised.

Cyber attack preparedness and response

The meeting began with a facilitated discussion about best practices in the anticipation of and response to potential cyber attacks. One moderator asked the participants if their institutions had ever experienced a cyber attack. The handful of hands that went up quickly came down when the moderator asked if those participants had the resources they needed to respond to the attacks. The moderator added that regulators can treat breached entities as defenders rather than victims, making it difficult for companies to know how best to respond to a breach.

Unfortunately, there is no single best way for organizations to prepare for a breach. Federal enforcement agencies have not defined a standard for preparedness. Such a standard would have to be flexible enough to account for diverse approaches to data management across different types of stakeholders and nimble enough to adapt to rapid changes in technology. Such an approach may simply be too difficult for a federal agency to undertake. Likewise, although a self-imposed, standard-setting industry organization that conducts audits could potentially ease the burden of preparedness, no single effort has emerged that organizations can follow to establish their policies. Instead, individual organizations are generally left to develop individual security protocols to limit the damage of a cyberattack and protect the enterprise from liability.

The aftermath of an attack

After a breach, law enforcement and federal regulatory agencies get involved to determine how the breach occurred. It is essential that privacy and security teams document all of the steps the organization took in systematically assessing risk, developing policies to guide incidence response, and responding to the breach to demonstrate robust efforts to safeguard patient data. "The government will look at what you did in the aftermath of a cyber attack," said one moderator. "Did you have a post-breach plan? Did you practice your plan? And after the breach, did you follow your own processes? Did you notify affected individuals? Did you provide credit protection?" The answers to these questions will determine how regulatory agencies assess an incident.

By planning and documenting ahead of an incident and routinely reassessing policies, organizations will be better poised to respond to a potential breach. It can also help to engage law enforcement and regulatory agencies to build strong working relationships with stakeholders and regulators and to determine what will be expected of an organization in the event of a breach. Several participants voiced a need for a self-imposed, standard-setting organization that conducts audits. Some organizations have begun to do this, but no single one is in the driver's seat of this effort.

Practice makes perfect

Another essential preparedness strategy is to routinely test response policies by practicing with simulated events. Conducting tabletop exercises and live simulations can help identify vulnerabilities, both in systems and processes. One participant recommended conducting both tabletop exercises and live simulations to test a company's vulnerability and readiness for a breach. In tabletop exercises, a company's incident response team talks employees through an escalating incident scenario, requiring the team to create a plan of action to address the scenario at various stages. Live simulations are unplanned, requiring responders to detect and respond to an unfolding staged scenario.

One attendee said his company has conducted such exercises, and that was where "the rubber hit the road." "It's eye-opening," he said. "You realize that the contracts you have with your business partners play a big role in how

you communicate a breach. Having everyone in one room opens eyes as to where all the workstreams are and where there is room for improvement."

Simulations can also help organizations understand what to be vigilant for. Many breaches aren't sudden, obvious attacks on a system. Rather, they may unfold slowly, or reveal themselves in unexpected ways such as increasing numbers of calls presenting fraudulent claims.

Perhaps most important, simulations help elucidate the importance of building a strong organizational culture regarding security. "Security is only marginally a technological issue—it is foremost a *people* issue," said one participant. Practice exercises are important for defining roles in the event of an incident. They help to construct a clearer view of who can and should be making difficult decisions like whether to take important systems offline.

Guiding data-sharing at the federal level

The federal government has used a number of different strategies to support healthcare organizations that seek to share data among stakeholders. For example, enforcement agencies were recently granted authority to proactively audit an organization's security policies. Audits have revealed systemic issues that other organizations can learn from. Enforcement agencies are also striving to use discretion when assigning liability for security incidents. The problem, said one regulatory representative, is when systemic issues are detected *after* a breach. Organizations that make good faith efforts to prevent breaches will be more protected when they occur despite their best efforts. "When an organization is doing everything right," said the representative, "it shouldn't be punished."

Another regulatory representative added that agencies look carefully at whether organizations took measured steps to reasonably protect healthcare data. "Reasonableness is contextual," she said. "That's why documentation is so important. We need to see the thought process that went into a decision. Did they consider the environment and thoughtfully make a plan?" Regulatory agencies make a great deal of compliance and enforcement information available to the public to inform the industry about gaps in security policies that can result in enforcement activity.

- HIPAA Security Guidance
- FDA Proposed Regulations and Draft Guidance
- ONC Security Risk Assessment Tool
- ONC Guide to Privacy and Security of Electronic Health Information
- ONC Health IT Privacy and Security Resources
- ONC Health Information Privacy, Seucrity, and Your EHR

Another way that federal agencies have worked to support data sharing is through guidance. Recognizing the difficulty of establishing "safe harbors" for security incidents, agencies are instead highlighting best practices and sharing information to help organizations make appropriate choices when developing security policies. Examples of guidance efforts include work to translate NIST's cybersecurity framework into a more digestible format, sharing example scenarios to demonstrate good conduct and promoting multi-factor authentication approaches. Additionally, agencies have amended privacy rules like HIPAA to include more flexibility regarding sharing data with patients. According to a recent rule change, patients can now receive healthcare data over unencrypted channels like email if that is their preference.

One regulatory representative addressed the negative effects of overreacting to potential liability by blocking patient access to their records. The necessity of engaging patients and helping them manage their own care is increasing because of our aging population, said one representative. When security is so complicated people can't access their own data, no one wins.

Other observations and recommendations that emerged during the conversation include:

- **Responsible cyber attack prevention and response requires constant recalibration.** Regulatory representatives urged attendees to stay current with new technoloiges and process and to treat their preparedness plans as living documents than can adapt to new threats as they arise.

- **Enact "need-to-know" access parameters.** Not all employees need the same access to information. Scale employees' access to what is required to fulfill their job requirements and no more.

- **Take advantage of available resources.** Websites of federal agencies like the Office of the National Coordinator for Health IT (ONC) contain a number of resources for the industry, including accounts of enforcement activities, resources on preparedness, and recommended actions. An upcoming website will incorporate a new blog that will allow regulators to field questions from the industry about preparedness on a regular basis. "You should not have to make this up from scratch," said one representative. "When you develop your policies and train your employees, this gives you a way to show you've followed our recommendations."

- **Balance regulatory requirements.** States are free to set their own legal requirements for privacy and security, but doing so has resulted in a difficult to navigate landscape of diverse rules. Multi-state and national organizations are challenged to comply with many different state requirements. Recognizing the issue, ONC is meeting with state representatives to help them understand the implications of misaligned laws and provide guidance to those that would like to streamline their regulations.

- **Information sharing can *enhance* privacy and security.** Such was the sentiment of one regulatory representative, who said that always saying "no" to a given type of information sharing can prevent patient-centered programs from being successful. "There are going to be risks to any type of data sharing," said the representative. "We can't eliminate all of it as a consequence." The repersentative added that they believe in information sharing, but you always need to target what you share. To better understand this, he said, privacy and security professionals need to go "in the trenches" and truly understand their systems.

- **The view from the White House is expanding.** One government representative mentioned the White House's increasing efforts to encourage data-sharing within the healthcare sector. The first effort, **The Open Data Initiative**, was enacted in 2013 by way of executive order, and it covers technical and scientific research as well as healthcare data. The overriding emphasis of the effort is to make available the vast amount of data collected by the federal government so the public may make use of that data for the benefit of all citizens. A more recent White House effort to increase data sharing is the **Precision Medicine Initiative**, which was introduced in the last State of the Union address. This effort will create a large database to be made available to researchers for efforts such as mitigating negative environmental factors and treating infectious disease.

- **Data-sharing can open new business opportunities and improve patient care.** Two attendees shared the unique ways in which their organizations are sharing information. While one is using patient information contained in a vast database to offer new services, another is connecting hospitals statewide through the use of a common electronic health record (EHR), enabling them to be more proactive with preventive care and cut down on hospital admissions.

In the end, the attendees voiced a desire to continue to expand efforts to share data to everyone's benefit while also sharing best practices to keep that data safe and secure.

This sentiment was best summed up by a participant who shared a story about thier child, who required treatment in three different states, none of which were equipped to communicate patient information to one another. As a result, there was a significant duplication of costly tests, and now the child's medical and identification information is hosted on several provider systems across multiple states.

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