Executive Advisory Board on Privacy and Security Meeting

Washington, DC

June 18, 2015

eHEALTH INITIATIVE
Real Solutions. Better Health

TAKING PROACTIVE STEPS TOWARD SECURING PATIENT DATA

SETTING THE AGENDA

The eHealth Initiative (eHI) Executive Advisory Board on Privacy and Security met on June 18, 2015 in Washington, DC, for the sixth time to explore strategies and ideas 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 Federal Bureau of Investigation (FBI), the Food and Drug Administration (FDA), and the White House Office of Science and Technology (OST).

Discussions throughout the day covered a range of subjects, from dealing with the everyday security threats faced by healthcare organizations to evaluating the role that patient data security plays in national security. Several themes emerged, including the balancing act between providing patients with convenience and the necessity of ensuring the security of sensitive information. Participants also discussed the lack of a cybersecurity culture in the healthcare industry and the link between the security of patient health data and national security.

At the start of the meeting, the issue of safe harbor was raised more than once, with participants asking the federal representatives present if their agencies could help them develop effective controls to avert threats from foreign governments and outside entities. Other participants emphasized the need for the industry to share knowledge, adopt consistent standards, and devise a security strategy. Most agreed that any successful strategy would require unprecedented industry collaboration among multiple entities. One issue raised in previous meetings was raised again: how to educate organizations' boards of directors about cybersecurity threats that cannot be addressed by regulatory compliance alone.

THE STATE OF CYBERSECURITY IN THE HEALTHCARE INDUSTRY

The discussion began with some commenters noting that patients appear to be ambivalent when it comes to how their medical information is handled. One participant pointed out that daily reports of data breaches in multiple industries have desensitized consumers about the prospect of having their own personal medical information compromised. After all, in many industries, if an individual's information is stolen, established consumer protections mean that he suffers only minor consequences.

For example, when a criminal steals credit card information, the owner simply notifies the credit card company, is refunded for fraudulent charges, receives a new card, and bears no legal liability. Subsequently, people may assume that the risks associated with the theft of their medical data are relatively inconsequential. Several participant s affirmed this, saying that patients can erroneously assume that all healthcare organizations have safeguards in place similar to those of the banking industry's stringent security measures.

The reality, participants agreed, is that gaps in cybersecurity within the healthcare industry pose serious risks to patient safety at multiple levels. In fact, purposefully altered patient information can result in incorrect diagnosis and treatment—leading to potentially life-threatening consequences. Stolen medical data can also be used for fraud or extortion, or to submit false claims to Medicare or Medicaid for reimbursement.

Patients may erroneously assume that all healthcare organizations have safeguards in place similar to those of the banking industry's stringent security measures.

Participants also acknowledged that, like many patients, healthcare workers—including physicians—are frequently uninformed about the dangers posed when patient information is stolen or hacked. Most participants agreed that educating both patients and providers about the dangers posed by poor cybersecurity is key to protecting sensitive data. One regulatory representative emphasized that healthcare organizations should take responsibility for educating consumers about how to best protect their sensitive medical information.

Participants also lamented the immature state of cybersecurity in the healthcare industry. One participant noted that most security officers in healthcare organizations work under the auspices of an IT department. This can erroneously imply that cybersecurity is purely a technology issue and should be treated as such. Another participant discussed the superiority of cybersecurity practices in other industries as compared to healthcare. In the financial industry, said one participant, "companies have an understanding of risk built into their DNA. They have created a culture of safety and cybersecurity that every employee buys into. Healthcare has not."

A BALANCING ACT

Participants acknowledged the difficulty of balancing the clear benefits of sharing digitized patient information among providers and payers with the risks of doing so. For example, while electronic prescriptions can enhance patient safety by guarding against medication errors, they also make patient information available to a significant number of people and the systems they use. Aggregating data across multiple systems increases the risk that more comprehensive patient information will be compromised in a single attack.

By fostering a culture attuned to potential threats, organizations will be better able to identify their own weaknesses and thwart attacks before they occur.

Several participants noted that the convenience v. cost dilemma inherent in sharing digitized patient data may best be addressed by framing cybersecurity as a people issue rather than a technology issue. By fostering a culture attuned to potential threats, organizations will be better able to identify their own weaknesses and thwart attacks before they occur. To effectively avert and manage risk, said several participants, employees must understand their organizations' unique technical and social vulnerabilities, the true value of the data in question, and any proactive steps they can take to avoid an intrusion. Building a culture of cybersecurity, said one participant, requires time and resources that many organizations in healthcare have been unwilling to invest in to date.

PROACTIVE MEASURES

The FDA representative addressed the necessity of ensuring the security of medical devices against cyber-attacks and simple tampering. The most effective tool the industry has to address this danger, she said, is education. Providers must be better educated about potential threats to the proper functioning of medical devices—which may involve not only hacking into networks to steal data, but also tampering with devices to interrupt or reconfigure functionality. The representative recommended fostering a culture of prevention regarding medical devices—just as hospitals have fostered a culture of quality care by implementing mandatory procedural checklists and hand-washing regimens.

The representative informed the group that the FDA is now receiving classified security briefings and that the Centers for Disease Control and Prevention (CDC) and the Centers for Medicare and Medicaid Service (CMS) may be included in the future. The briefings include not only what the FDA can do on its own, but also how it needs to leverage assistance from the private sector. In fact, a new cybersecurity working group has been created to work with the private sector. The representative also mentioned the upcoming "Cyber Storm V," a Department of Homeland Security exercise that is designed to examine organizations' capacities to prepare for and respond to the potential effects of cyberattacks. Part of the exercise will inject stress into the healthcare system to the point of failure with the goal of putting together a playbook to respond to potential real-life events.

The representative recommended fostering a culture of prevention regarding medical devices—just as hospitals have fostered a culture of quality care by implementing mandatory procedural checklists and hand-washing regimens.

Finally, the representative stressed the importance of data collection and information-sharing within the industry. Many medical devices in use today were developed and manufactured in an age in which cybersecurity was not the pressing issue it is today. To respond to future threats, the representative said the FDA needs more information on how malicious agents are attacking devices. In particular, the agency would like to see the healthcare industry reporting "near misses" that can help expose device vulnerabilities. Near misses, said the representative, tend to go unreported, due to fears of liability or regulatory reprisal. She assured the group that the FDA has pathways for submitting such data confidentially. One participant from a payer organization affirmed that his company has successfully worked with the CDC and partnered with the FBI and state agencies to prevent fraud.

THE GLOBAL GENOMIC ARMS RACE

When discussing threats to the security of healthcare data, many stakeholders tend to focus on immediate dangers in the form of hacking, fraud, or extortion. The representative from the FBI said his agency takes a more long-term view.

Dependent as it is on genetic sequencing, personalized medicine is changing the way medicine is practiced worldwide. As more medical data is captured, it is being analyzed on a population level to identify the molecular differences that contribute to a treatment's success. Currently, said the FBI representative, the healthcare system is still figuring out how to best manage and use all of the genomic data being generated across the globe. The entity that first determines how to unlock the potential of aggregated healthcare data for personalized medicine will have a huge advantage in commoditizing our "biofuture." Unfortunately, said the representative, it is increasingly looking like that entity might not be American.

The FBI representative said that by methodically amassing huge amounts of healthcare data through both legal and potentially illegal means, China has accumulated longitudinal medical records, personnel data, and other information on millions of US citizens. Put together, this data can offer an unparalleled view of the genetic functioning of the human being. Furthermore, the representative pointed out, the Beijing Genomics Institute (BGI) is the world's largest genome sequencing company, potentially able to access genomic data from millions of people across the globe. As the largest genomic clearinghouse, BGI does not have to resort to nefarious means to acquire data; many of the premier research institutions in the US voluntarily contract with BGI to meet their sequencing needs.

Losing the race for our biofuture could place the US at a distinct economic disadvantage, and even threaten our national security by making us unable to adequately respond to new infectious diseases or bioterrorism.

By combining this wealth of data with advanced analytics, said the FBI representative, China is well-poised to make the types of breakthroughs necessary to unlock the world's biofuture. Already, China likely possesses enough data to gain a significant competitive advantage in pharmaceutical research and development—a process that can take decades and cost companies billions of dollars in the US.

Moreover, said the representative, Chinese companies are not hindered by the regulatory and legal mechanisms that protect patient privacy in the US. China is also investing heavily in developing an analytics workforce with the skills to make use of its large genomic data sets. Losing the race for our biofuture, said the FBI representative, could place the US at a distinct economic disadvantage, and even threaten our

national security by making us unable to adequately respond to new infectious diseases or bioterrorism.

VIEW FROM THE WHITE HOUSE

The representative from The White House Office of Science and Technology (OST) acknowledged the importance of accumulating and leveraging data to drive new understanding of healthcare trends across demographic groups. For example, big data analysis can facilitate new insights into why certain populations are more susceptible to different pathogens, or why they respond better to specific vaccines.

While a single medical record was worth $300-$330 on the black market in 2014, it has jumped to a $1,100 —far outpacing the price of stolen debit cards and PIN numbers

The OST representative stressed the need to enable widespread access to healthcare data sets within parameters that ensure information is not misused. Unfortunately, today's analytic tools are growing powerful enough to enable malicious agents to target individuals within a data set. Although various pieces of federal legislation work to protect consumer privacy, said the representative, there is still no comprehensive regulatory framework that can guarantee to consumers that their data is secure and their identities are protected. Until such a fail-safe methodology exists, concluded the representative, organizations have to rely on restricting access to data sets to trusted parties.

FINAL THOUGHTS

During the meeting's final discussion, one participant noted that stolen medical records on the black market are spiking in price. He said that while a single medical record was worth $300-$330 on the black market in 2014, it has jumped to a $1,100 —far outpacing the price of stolen debit cards and PIN numbers. The participant said the skyrocketing demand for stolen medical records underlines the fact that current privacy laws are inadequate, and that stakeholders in the public and the private sector need to work together to better secure sensitive patient information.

Another participant warned against focusing data security measures solely on breach prevention, noting that the issue encompasses much more than that. At the same time, she added, she didn't want to scare her board into not sharing any patient information with other entities. "We need to help our board understand the true value of information sharing," she said, "as long as the necessary precautions are taken."

Another participant noted that too much is at stake for the US to lose the data arms race to China or any other country. The regulatory representatives agreed, stressing the value of the exchange of information between the federal government and private sector.

Ultimately, the group agreed that the security issue they are facing is ultimately a people issue in that it is ultimately people—not technology—who allow data to be compromised. Shoring up their employees' knowledge of how to safeguard the information that passes through their hands each day can be the best defense against compromised patient data.