# Executive Advisory Board On Privacy And Security

## Healthcare and Cybersecurity

November 12, 2014

eHEALTH INITIATIVE
Real Solutions. Better Health.

# Executive Summary

On November 12, 2014, representatives of the payer, provider, and pharmaceutical industries and of four federal regulatory agencies gathered in Washington, DC, for the fifth gathering of the eHealth Initiative (eHI) Executive Advisory Board on Privacy and Security. The chief information security officers (CISOs), chief privacy officers (CPOs), and other c-suite executives who make up the Advisory Board had previously met four times to discuss their top privacy and security concerns and best practices to protect sensitive patient information. During this meeting, the group concentrated on addressing the increasing cybersecurity risks across the healthcare sector.

The group recognized that, when they are successful, today's threats can wreak havoc among healthcare organizations, as evidenced by several high-profile, well-publicized security breaches that have occurred just during the past year. Hackers now seek patient data as much as—or more than—financial information. It is no longer an issue of *if* there's a breach, but rather *when* a breach will occurs. This new reality necessitates an everyday, common-sense approach to managing risk and protecting data.

The industry and regulatory representatives at the meeting discussed how the ubiquity of digital information in the healthcare sector means that the number of individuals who have access to sensitive patient data is growing exponentially. Industry representatives agreed that they have a mutual interest in protecting their sensitive information, and they could gain much by working collaboratively to guard against cybersecurity threats to their industry.  Regulatory representatives noted that they see some awareness of this within the industry, but many remain hesitant to collaborate with their competitors.

Participants discussed the need for a secure platform that would enable healthcare information executives to share with one another their organizations' intelligence on cybersecurity threats and best practices. They recognized that other business sectors have managed to do this and affirmed that it is possible within the healthcare sector as well.

# Introduction: New cybersecurity threats demand industry response

At the start of the meeting, representatives from PwC defined cybersecurity as the safety of electronic access in an increasingly interconnected world. Potential cyber threats, said Mick Coady, principal at PwC, can take a variety of forms, including foreign nation states, organized crime groups, and "hacktivists."

"There has been an increase in these specific groups targeting healthcare," affirmed Coady. "In the past, there were non-specific employee and contractor threats (i.e., "insiders") that were largely unorganized and sometimes unintentional."

When they are successful, today's threats can wreak havoc among large retailers, banks, and healthcare organizations, said Coady, as evidenced by several high-profile, well-publicized security breaches of US companies that have occurred just during the past year. "Today's cyber-threats are organized, highly motivated, well-funded, and persistent," said Coady. "And they require an equally organized response to counter them."

The ubiquity of digital information means that the number of individuals who have access to sensitive data is growing exponentially—often without the knowledge of the people who generated and have a responsibility to protect that data. "Everything we do now digitally is connected to cloud-based platforms," said Coady. "Boundaries are gone. We may be completely unaware that our vendors are offshoring tasks—our information could be going out of the country with no safeguards and without our knowledge."

And yet we want—and need—to freely interact with data on a daily basis.

As we move toward a more interconnected world, it becomes increasingly important that we strike the right balance between necessary access and protective safeguards. The question is, how do we get there?

## Building a collaborative effort

The group reached significant consensus regarding the importance of cross-industry, intra-industry, and public/private collaboration in effectively addressing the mutual problems caused by threats to data security. Because all data will never be truly secure from prying eyes and parties with malicious intent, participants agreed that they need to be able to share with one another lessons learned and common defense mechanisms to protect their individual companies from what can be the devastating fallout of a security breach.

"We find that we are dealing with the same issues as our competitors," said one participant. "Vendor management, new entrants, pop-up companies—if we can't have a forum on these topics, it will be a detriment to the industry."

Other participants noted that collaboration seems to be particularly difficult for the healthcare industry. "The financial industry realized the value of cross-industry collaboration long ago," said one participant. "We also need to recognize how much we have to gain by working together as an industry and with regulators."

"There is a tendency and culture not to share data within healthcare," added Coady. "Legal departments tend to shoot down security executives when they want to hold discussions with their competitors. This is not an IT barrier—it's a cultural one."

# Regulators' viewpoint: The state of the industry

Representatives from the Office of the National Coordinator for Health Information Technology (ONC), the Office of Civil Rights (OCR), the Food and Drug Administration (FDA), and the National Institute of Standards and Technology (NIST) joined the Advisory Board to discuss the role and effectiveness of cybersecurity in the healthcare sector.

The regulatory representatives presented an optimistic view of the state of the industry's collaboration on privacy and security issues. Representatives said that they perceive the public and private sectors as beginning to coalesce as a community rather than point fingers and assign blame. Public-private sector collaboration is critical to solving problems, said the representatives. It is no longer an option to think about cybersecurity as the "other guy's problem." There is a new level of acceptance that all industry players need to take on shared responsibility for dealing with privacy issues.

Many federal agencies view cybersecurity as an evolving issue. Groups like the FDA are encouraging organizations to recognize that they can make progress by first tackling obvious, easily addressed security risks. To help the industry identify those risks, the FDA is fostering collaborative approaches to security with the private sector. The agency has participated in outreach activities to help companies identify their specific vulnerabilities. Specifically, the FDA is working to increase awareness of cyber threats and identify tools and frameworks to encourage the public and private sectors to work together.

For example, the FDA spends time educating the public about the consequences of poor cybersecurity measures and breaches. Currently, very few hospitals are adequately aware of the extent of their cybersecurity risks. Although there is a greater awareness among organizations that the industry needs to better collaborate, there are very few examples of that collaboration actually occurring.

The group also discussed the extent to which patient data is at risk in the healthcare sector and how that relates to an organization's size. For example, smaller practices may invest in EHRs, but not in securing the patient information that they digitize. In many hospitals, there is still a lack of understanding about basic security safeguards.

The representatives noted, however, that having a large business does not always provide sufficient protection against breaches. It is helpful to emphasize the critical role of cybersecurity to healthcare organizations, by helping them understand what might happen to their reputations if their patients' personal information is compromised on the same scale as recent retailer breaches.

The regulatory representatives agreed that it is important to start addressing risk by concentrating on the "low-hanging fruit" that offers healthcare organizations the opportunity to quickly secure information at high risk—such as the data on mobile devices and data "at rest." Todays' cyber environment, necessitates an everyday, common-sense approach to managing risk and protecting data.

## Breaches happen

The regulatory representatives also acknowledged that, in spite of the best efforts to protect data, some breaches will happen. They also said that one way companies can best protect their interests is by adequately documenting their security measures. The representatives urged healthcare organizations to create and document a culture of compliance and a common-sense approach to ensure that their patient information is appropriately safeguarded. These documented procedures,should not be on the shelf collecting dust. Such procedures should ensure that no employee has access to information that he or she doesn't need to see, and that private health information is disposed of securely.

The regulatory representatives encouraged organizations to take a reasonable and prudent approach to cybersecurity. Participants were told that the OCR does not view itself as a policing entity. The OCR does not use audits as an enforcement tool; rather, they are a learning tool. OCR takes a voluntary approach to compliance, even when taking a corrective action. Participants were encouraged to examine the OCR's online audit protocols to determine if they have taken appropriate cybersecurity measures and have sufficiently documented those measures so they could pass a possible audit.

The participants were also told that the ONC is not in the business of security enforcement. Rather, the agency takes a practical approach to cultivate privacy and security awareness in the healthcare sector. The ONC provides resources to help healthcare organizations integrate privacy and security measures into their organizations. The agency focuses its efforts on small-scale providers to help them enhance the security of their patient information.

## Combating cybersecurity risks with regulatory tools

The group also learned that some of the ONC's most popular resources are its recently launched privacy and security virtual training games.[1] Created especially for small practices that may be unfamiliar with all of the Health Insurance Portability and Accountability Act's (HIPAA's) rules and regulations, the ONC's security training gaming module asks users to respond to the privacy and security challenges most often faced in a typical small medical practice. Users choosing the right responses earn points and see their virtual medical practices flourish. Users who make poor security decisions see their practices suffer the consequences.

The regulatory representatives said ensuring that small practices are up to speed on the most effective security protocols is vital, as these medical offices can be the gateway through which security is most likely to be breached.  An example was given of a patient in a high-deductible health plan who uses his debit card to pay for medical services. Many small practices cannot guarantee the safety of a simple debit card swipe. Representatives agreed that healthcare organizations need to make sure financial transactions in medical offices are safe, saying that it is critical that patients can trust individual, micro-transactions.

[1] Privacy and Security Training Games, HealthIT.gov (http://www.healthit.gov/providers-professionals/privacy-security-training-games)

All of the regulatory representatives present referred to the privacy and security "frameworks" their respective agencies have developed or are in the process of developing. For example, the National Institute of Standards and Technology (NIST) at the US Department of Commerce educates healthcare organizations about the Framework for Improving Critical Infrastructure Cybersecurity, which was released in February 2014.[2]

The framework was created in response to an Executive Order issued by President Barack Obama in 2013, which called for "the development of a voluntary, risk-based cybersecurity framework—a set of industry standards and best practices to help organizations manage cybersecurity risks." The framework was developed in concert by the government and private sector, and it attempts "to address and manage cybersecurity risks in a cost-effective way based on business needs without placing additional regulatory requirements on businesses." It brings together the standards, guidelines, and practices that are working effectively in industry today so that all sectors and entities may benefit from them.

The frameworks are voluntary and are not intended to compete with existing standards. Rather, they are meant to be common communication tools that can help organizations align their security efforts. The representatives present said they embrace the development of these frameworks because of their longer shelf life. The focus, they said, should be on awareness and outreach, and frameworks can support that work.

## Responding to vendor challenges

Another common theme among the cybersecurity concerns that the Advisory Board discussed with regulators was concern about the privacy and security knowledge and capabilities of business vendors. "A major limiting factor is the lack of awareness among vendors," said one participant. "Many are running on obsolete, end-of-life infrastructure."

The problem is not limited to small-scale vendors, added another participant, drawing attention to a major EHR vendor that is unable to encrypt databases. "All of our patient information is in our database," he said. "We put compensating controls around it, but the basic capabilities are not there; it would be far better if the vendor could do it."

Another participant expressed frustration that some vendors do not even install simple anti-virus software on their products. But such concerns, he said, are not sufficient for him to object to the product if business needs dictate the need for it. "Business needs are going to trump security every time," he said.

Several participants brought up the possibility of developing a proactive effort within the industry to expose vulnerabilities in vendors, so that when one organization determines that a vendor's security measures are insufficient, other organizations can be alerted to that finding. "We all agree this is a problem," he said, "the issue is coming together to create solutions."

Organizations that find security vulnerabilities in their vendors' products should document those vulnerabilities and then lean on vendors to implement best security practices. Vendors should make the same security investments as healthcare organizations are. If business

[2] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014. (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf)

associates are not compliant, healthcare organizations should notify the appropriate regulatory agencies.

“We all in our own businesses hold the power of the purse,” said one participant. “And we need to take advantage of that. Do site visits on your vendors. How are they physically securing their buildings? How do they dispose of paper? Make sure your vendors know what the consequences are to *you* if they have a breach.”

The FDA issued new guidance in October 2014 on the content of premarket submissions for medical devices regarding their cybersecurity.[3] The guidance aims to help the healthcare industry identify cybersecurity issues that manufacturers should be taking into account when designing and developing medical devices. While the guidance is non-binding, new medical devices submitted to the FDA for approval will be evaluated based on the requirements outlined in the guidance document. Products that do not meet those requirements will not be approved for use.

The FDA is looking to the industry to help address vendor concerns. One participant said that he knows of one healthcare system that has established privacy and security requirements that its vendors must meet before the system agrees to purchase a vendor’s product.

PwC’s research illustrates that. Of the healthcare security, IT, and business executives who participated in the firm’s 2015 Global State of Information Survey, only 62% have a program to identify sensitive assets, and only 60% say they have conducted an inventory of all of the third parties that are authorized to handle the personal data of their employees and customers.

## THE STATE OF INFORMATION INSECURITY

PwC’s recently published Global State of Information Security Survey (GSISS) revealed some worrisome trends in privacy and security in American industry as a whole and in the healthcare sector in particular.[4] The number and cost of security incidents in the healthcare industry continues to soar. The responses of healthcare payers and providers responding to the survey indicate that the number of security incidents in the sector in 2014 increased 60% over 2013, an increase that was almost double the number of incidents reported by all other industries.

The cost of these breaches is also increasing. The estimated average financial loss as the result of a security incident rose to $2.9 million in 2014, 282% higher than in 2013. And more valuable data is being targeted. Survey respondents reported that identity theft jumped 32% compared to last year, and 20% of respondents said personally identifiable information was compromised in their organizations.

[3] US Department of Health and Human Services, “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff,” October 2, 2014. (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf)

[4] PwC, “The Global State of Information Security Survey 2015.” (http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#)

Joe Greene, a principal at PwC, pointed out that the ultimate number of security breaches and economic fallout will never be known, as many security events go undetected and/or unreported. “And despite these risks,” said Greene, “spending on information security is modest.” Information security spending as a percentage of IT budgets in the industry was 3.4% in 2013 and 3.7% in 2014. “If IT budgets aren’t growing, security budgets aren’t growing,” said Greene. “Security budgets should not be tied to IT spending.”

## Action starts at the top

In spite of the increased risk to patient information indicated by a skyrocketing number of security breaches, Greene said most healthcare organizations have not elevated security to a board-level discussion. “As a result,” he said, “leadership is not supporting key privacy and security initiatives.”

Only 25% of survey respondents said that their boards of directors participate in reviewing current security and privacy risks. Just 24% of boards are involved in decisions regarding security technologies, and 32% participate in developing security policies. “Top-down commitment to and participation in security concerns is crucial,” said Greene. “Senior executives need to ensure that boards understand what risks an organization faces and how best to respond to them.”

All regulatory representatives agreed that one of the most effective ways executives can help prioritize privacy and security measures in their own organizations is to obtain support at the top. Representatives said that common-sense protections can provide vigilance on a day-to-day basis, and that company leadership should emphasize the importance of being aware of security practices. The c-suite should convey that compliance is as important to a company’s success as marketing and quality. Privacy and security are too often pushed down the list of company priorities in degree of importance.

Several participants said that their boards have begun to voice concern about the privacy and security of patient information. “My board is active and interested,” said one participant. “I think they are there at understanding the cybersecurity concerns. They are asking questions, but they don’t have the answers. That’s where we can come in.”

“We see boards take interest in cybersecurity, but they don’t know how to implement solutions,” said Greene. “As boards mature in this area, they will provide another oversight level. We are trying to shorten that time.”

# Final thoughts: Practical steps forward

In summing up the day’s discussion, participants exchanged ideas about how to increase industry cooperation to develop solutions to cybersecurity threats. There are some indications that this collaboration is already occurring. Fifty-six percent of the healthcare executives responding to the GSISS said that they were collaborating with industry colleagues to decrease their cybersecurity risks. While this is a positive trend, participants noted that “collaborating” may mean different things to different people. While one executive may believe that placing a few phone calls to colleagues at other organizations constitutes collaboration, another may be participating in a formalized information-sharing forum.

Participants agreed that while they hear objections to collaboration on the grounds of not wanting to share proprietary information, disclosing sensitive company information is not a prerequisite for collaboration on security concerns. "We meet with our competitors in a law firm to discuss these issues, so it's all under attorney-client privilege," said one participant. "We are constantly bouncing questions off one another regarding what controls we have implemented and if our controls have worked. We all have our trade secrets that we don't want to disclose, but we don't have to do that in order to collaborate."

Participants also brought up the idea of sharing intelligence with their competitors when they are personally attacked in an effort to minimize damage to the industry. One participant said that his organization had benefited from a warning provided by a competitor shortly after that competitor detected a breach. "That allowed us to have a leg up on the attack to protect ourselves from damage," he said. "If that had happened to my organization, it would not have occurred to me to let my competitors know. It taught me that we should always keep in mind that we are part of a larger network.'"

Other practical considerations that participants suggested included the need to create information-sharing standards across the industry. "Everyone says they want to collaborate, but they struggle with the forum in which to do so," said one participant. Creating that forum is important, he said, but organizations should not wait to talk to one another. "Any kind of collaboration is desirable," said the participant. "We need to do it today."

In the long-term, though, processes and details will need to be ironed out and agreed upon. "We need to have a common platform and legal agreements on sharing information to make long-term collaboration with our peers work," said one participant. And larger organizations need to realize that a return on such investments make take a while to materialize. "Large organizations need to recognize that they are not going to get equal benefit from their leadership efforts," said one participant. "It will benefit them in the long-run, but they must first provide the primary leadership."

Another concern is how to process all of the information that will be gained from industry collaboration. "Very few companies have made the investment needed to digest the huge amount of information they would receive through their collaborative efforts," said one participant.  Others agreed that this will be another problem looming on the horizon once they can get their companies to start a meaningful dialogue with one another. "How do we create an infrastructure to exchange data, allow for a high level of collaboration, and then process the information we obtain?" ask one participant.

In the end, the group reached significant consensus regarding the importance of cross-industry, intra-industry, and public/private collaboration in effectively addressing the mutual problems caused by threats to data security. Because all data will never be truly secure from prying eyes and parties with malicious intent, participants agreed that they need to work on a framework that would allow sharing with one another lessons learned and common defense mechanisms to protect their individual companies from what can be the devastating fallout of a security breach.

The Advisory Board will meet again in Washington, DC, on March 3, 2015 to review their progress and continue dialogue with industry regulators to address privacy and security threats in the healthcare sector.

# eHI Executive Advisory Board on Privacy & Security

## Acknowledgments

Aaron Lewter, Information Security Officer, Manager of Networks and Security Services, Availity

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

Carl Anderson, JD, Vice President, Van Scoyoc Associates

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

Cris Ewel, Chief Information Security Officer, Seattle Children's

Daniel Nutkis, Founder & Chief Executive Officer, HITRUST Alliance

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

Guy Turner, Chief Data Security Officer, Sutterhealth

Hans Keil, Chief Information Security Officer, PerkinElmer

Jennifer Covich-Bordenick, Chief Executive Officer, eHealth Initiative

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

Jon Moore, Chief Information Security Officer, Humana

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

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

Kevin Charest, Senior Director, IT Threat Intelligence, UnitedHealthcare

Matthew Lawson, Director, Cybersecurity and Privacy, Health Industries, PwC

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

Mick Coady, Partner & Co-leader, Cybersecurity and Privacy, Health Industries, PwC

Nikolay Chernavsky, Director of Information Security, Amgen

Norberto Robles, Chief Information Officer, New York City Health and Hospitals Corporation

Pamela Arora, Chief Information Officer, Children’s Medical Center

Ralph Lange, Director, Enterprise Infrastructure, Availity

Robert Booker, Chief Information Security Officer, UnitedHealthcare

Sara Juster, Associate General Counsel & Privacy Officer, Surescripts

Thien Lam, Chief Information Security Officer, BayCare Health System

Thomas Baltis, Deputy Chief Information Security Officer, Blue Cross and Blue Shield of IL, TX, NM, OK, MT

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

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