EXECUTIVE ADVISORY BOARD ON PRIVACY & SECURITY

PRIVACY, SECURITY, & COLLABORATION IN OUTCOMES-DRIVEN HEALTHCARE

eHEALTH INITIATIVE
Real Solutions. Better Health.

Introduction

New regulations are presenting fresh challenges to healthcare privacy and security executives. As the healthcare industry continues to struggle to achieve and maintain compliance with existing regulatory requirements, new regulations are pending, and newer ones are on the horizon. The HIPAA omnibus regulations and evolving meaningful use requirements for electronic health records (EHRs) are two of many governmental initiatives that are increasing the regulatory burden on healthcare organizations. As EHRs become more operational and widespread, the exchange of health information will increase exponentially, making privacy and security an even more important component of the overall healthcare IT ecosystem.

The Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health IT (ONC) continue to issue new privacy and security regulations, standards, and guidance; it is becoming increasingly apparent to healthcare organizations that focusing their attention on privacy and security from a strategic perspective makes sense. New technologies (mobile devices, social media, and telehealth) and advancements such as health information exchange, accountable care organizations, and data and predictive analytics make it critical for organizations to make privacy and security an essential component of their overall clinical and business practices. As patients become more aware of the ability of organizations to move their personal healthcare information among multiple industry stakeholders, they may take the security of that information into account when determining where to access healthcare. Organizations that have recognized this have gone beyond viewing security as a regulatory requirement and have embraced it as an opportunity for competitive advantage. In May 2013, eHealth Initiative (eHI) convened a multi-stakeholder Executive Advisory Board on Privacy and Security in Washington, DC. The board, composed of chief information officers, chief information security officers, chief privacy officers, and other c-suite level executives from the healthcare sector, met to discuss their top privacy and security concerns and identify solutions to common problems. Their differing perspectives provided valuable insight into the challenges and opportunities the industry is facing and offered a glimpse into the direction of the industry at a time of significant change. This paper identifies some of the key considerations the board raised.

Key Considerations Identified

- **Clarity** – It is important to strike a balance within the regulatory privacy and security framework to allow for innovation while being prescriptive enough to ensure that compliance requirements and goals are clear.
- **Primacy in privacy** – Privacy and security should be integrated into healthcare organizations' strategic goals and daily clinical and business workflows to foster a culture of privacy.
- **Consumerization of health information** – As health information is increasingly digitized, patient access, use, sharing, and transmission of information has become easier. It is important to educate patients about the opportunities created by these changes and the potential consequences of sharing their data.

- **Organizational culture** – A cultural shift is necessary to think outside the traditional siloed approach to privacy and security and collaborate with others to addressing common privacy concerns.
- **Small providers** – Although they have limited resources, smaller providers and healthcare organizations must meet the same privacy requirements as larger organizations. These smaller organizations can leverage materials developed by the government to assist them in their efforts to approach privacy and security strategically.

MOVING FORWARD

During a lively discussion, advisory board participants identified a range of key issues and potential solutions that should be top of mind for today's leaders in the healthcare IT sector. The board agreed that private and public healthcare leaders must work together to address these issues as emerging technologies continually shift the privacy and security landscape. To move forward in addressing the issues and challenges of their industry, the board articulated these chief areas of concern that warrant immediate action:

Cultivating clarity: Participants expressed the real importance of flexibility and clarity in ongoing governmental regulations, guidance, and materials that demonstrate the future direction of privacy and security. They agreed that the government's responsibility is to craft policies that not only foster innovation, but also are workable in practice and do not needlessly break the bank. To do this, government must strike a balance. Too much ambiguity in regulations can result in divergent interpretations, making implementation difficult. However, prescriptive approaches may not be practical for a wide variety of technical infrastructures and health systems. The group believed that regulatory agencies shared the goals of flexibility and clarity. The question is, how do we improve this path going forward? This is especially compelling given the increased complexity of health care, and how it is evolving-- the need to explore new business models, bring down costs, better engage with patients, and improve health outcomes.

The board agreed that the recently released HIPAA omnibus rule is an example of challenges in reaching clarity and increased burden. The broad spectrum of interpretation this regulation spawned has made implementation difficult. The HIPAA omnibus rule requires significant changes in several operational areas that impact organizations, including:

- **Business associates** – A new definition of a business associate (BA) now encompasses a variety of subcontractor organizations that weren't previously classified as BAs. Downstream contractors from BAs that touch protected health information (PHI) will now be considered BAs themselves.
- **Personal medical information** – Providers will no longer be permitted to share personal medical information with insurance companies for services a patient pays for out of pocket. The challenge is to develop technology that supports this requirement in time.
- **Medical records** – Provisions were removed that permits 60 days for retrieving and copying a record that is maintained off site. The covered entity has 30 days with one-time 30 day extension to respond to the request (with the written notice to the individual of the reasons for delay and expected completion date). This provision extends the 30-day time limit with a one-time 30-day extension to respond to requests for electronic access. This aligns the time period to respond, no matter the location or the media.
- **Pharmaceutical communications** – With some exceptions, the final rule requires patient authorization prior to using PHI for all paid communications recommending a product or service to the patient.

The board expressed a desire for frequent communications from regulatory agencies, including overview documents, online games and scenarios, competitions, and town hall meetings. Before regulations or guidance are issued, regulatory agencies should explore ways to dialogue with organizations so that flexibility and clarity can be achieved. The group also suggested a tactic employed by the IRS and financial sector: private letter rulings (PLRs). A PLR is a written statement in response to a request submitted by a taxpayer that interprets and applies tax laws to the taxpayer's represented set of facts. Organizations could use PLRs to promptly receive answers on specific interpretations related to their unique situations.

Achieving primacy in privacy: With the accelerating pace of technology, privacy has become a challenge for all industries. The sensitive nature of the patient information healthcare organizations transmit each day raises the stakes when it comes to potential data breaches in this sector. Board members agreed that organizations often unwisely address privacy and security requirements as a separate component that can impact the adoption and implementation processes. Approaching privacy and security from this perspective can work against fostering a culture of patient safety. For example, rather than address privacy and security as foundational requirements for meaningful use, the federal government addresses them as separate elements within the overall EHR certification program. Board members emphasized that providers and healthcare organizations should integrate privacy and security into their day-to-day clinical and business practice workflows, making them seamless with other IT functions.

Embracing consumerization: As health information becomes more digitized and thus less challenging to access, electronic data is becoming more consumer-friendly, making it easier to use, share, and transmit. Board members agreed that providers and other healthcare organizations should continually modify their privacy and security policies to keep up with evolving trends in patient access. It is important that organizations take on the responsibility of educating providers about data use, access, control, and the potential risks of sharing health information in an unsecured environment. They should create awareness about the opportunities offered by increased access but also balance it by emphasizing the need for patient education. Healthcare organizations should cultivate trust in their systems so consumers do not have a reason to question the security of their health information as it is transmitted across the continuum of care. This is especially important with new meaningful use rules that require providers to make patient PHI available to a wide variety of users, from public health agencies to individual patients themselves.

Transforming organizational culture: The board discussed approaching privacy and security as an integral and foundational element of an organization's overarching strategy, making patient privacy part of the continuous improvement process. For this to happen, a culture shift needs to originate at the top of an organization: Leaders must promote privacy and security as opportunities to improve patient care, rather than as separate, onerous requirements that must be met. Rather than viewing privacy requirements as punitive, organizations should focus on how they can use them to create a positive patient experience.

Some providers have bucked traditional corporate culture by actually joining forces with their competitors to meet their mutual privacy needs, in an appropriate manner considering anti-trust and other rules. These erstwhile rivals agree not to compete on security. Instead, their information security officers share ideas, discuss challenges, and synchronize their approaches to address emerging privacy concerns. Incorporating community-wide approaches into the overall culture of individual hospitals is also important, as many providers in a given region are community-based.

Assisting small providers: Small providers need to meet the same privacy requirements as large providers — however they are allowed to have scalable approaches in order to meet the baseline privacy and security standards. Additional controls can be implemented by professionals based upon an organizations business models, risk assessments, and operational capabilities. The board discussed the significant challenges that small organizations are facing as they struggle to achieve compliance with privacy and security regulations. The regional extension center program, which was created to help small providers implement compliance solutions, has met with mixed success. The government recently released new materials for small providers, such as the security awareness game and video, which focuses on basic steps that providers can take to improve security within their organizations. With their limited resources, small providers would do well to implement the leading practices recommended for organizations of all sizes, approaching privacy and security from a strategic vantage point and embedding it into everyday processes.

FINAL THOUGHTS

It is clear from the board's discussion that much work remains. The board agreed that private and public sector leaders must continue to communicate and work together to address the multiple concerns raised by the ongoing regulation of privacy and security. eHI will convene the board again in late 2013 to delve deeper into the challenges identified here and to address the next steps in navigating the ever-changing healthcare regulatory landscape.

eHI Executive Advisory Board on Privacy and Security Acknowledgments

Jennifer Covich Bordenick, Chief Executive Officer, eHealth Initiative

Mick Coady, Partner & Co-Leader, Health Information Privacy & Security Practice, PwC

Mike Cunning, Director, PwC

Myra Davis, Senior Vice President, Chief Information Officer, Texas Children's Hospital

Dan Garrett, Principal and Health Information Technology Practice Leader, PwC

Nalneesh Gaur, Director, PwC

Trent Gavazzi, Senior Vice President and Chief Technology Officer, Availity

Joseph Johnson, Chief Information Security Officer, CHS Health Services

Bryan Kissinger, HIPAA Leader, Kaiser Permanente

Mark Lantzy, Chief Information Officer, WellCare

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

Deven McGraw, Director of the Health Privacy Project, Center for Democracy & Technology

Ronald Mehring, Director, Information Security, Texas Health Resources

Mitch Parker, Chief Information Security Officer, Temple University Health System

Joy Pritts, Chief Privacy Officer, Office of the National Coordinator for Health IT

Dan Rode, Vice President, Advocacy and Policy, American Health Information Management Association

Laura Rosas, Program Analyst, Office of the National Coordinator for Health IT

Zoe Strickland, Vice President, Chief Privacy Officer, UnitedHealth Group Incorporated

Tim Thompson, Chief Information Officer, BayCare Health System

Amanda Titiliuc, Chief Information Officer, Summit Medical Group

Micky Tripathi, President and Chief Executive Officer, Massachusetts eHealth Collaborative

Allison Viola, Vice President, Policy and Government Affairs, eHealth Initiative

Heather L. Wojcik, Manager, PwC