CHiME

Testimony before the United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Health

Hearing on “Examining Cybersecurity Responsibilities at HHS”

2123 Rayburn Office Building

May 25, 2016

Statement of Marc Probst

Vice President and Chief Information Officer, Intermountain Healthcare

Board of Trustees Chairman, College of Healthcare Information Management Executives

Thank you, Chairman Pitts, Ranking Member Green and members of the subcommittee. It is an honor to be here today to testify on behalf of the College of Healthcare Information Management Executives, or CHIME, concerning the relationship of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) at the Department of Health and Human Services.

CHIME is an executive organization serving nearly 1,900 CIOs and other senior health information technology leaders at hospitals, health systems and clinics across the nation. CHIME members are responsible for the selection and implementation of the clinical and business technology systems that are facilitating healthcare transformation.

In addition to serving as chairman of the CHIME board of trustees, I am CIO and vice president for information systems at Intermountain Healthcare in Salt Lake City, Utah. Intermountain is a nonprofit integrated health system that operates 22 hospitals in Utah and Idaho; more than 200 clinics; and an insurance plan, SelectHealth, which covers approximately 900,000 lives in Utah and Idaho. Additionally, Intermountain Medical Group employs approximately 1,600 physicians, and about 4,000 other physicians are affiliated with Intermountain. Intermountain has over 36,000 employees.

Nationally, Intermountain is known for providing high quality care at sustainable costs. One way we achieve this is by identifying best clinical practices and applying them consistently. Research reviewed by John Wennberg, M.D., director emeritus of the Dartmouth Institute and founder of the Dartmouth Atlas of Health Care, showed that "Intermountain is the best model in the country of how you can actually change health care for the better." Dartmouth estimated that if healthcare were delivered nationally in the way it is provided at Intermountain, "the nation could reduce health care spending for acute and chronic illnesses by more than 40 percent." Essential to Intermountain's ability to deliver high-value coordinated patient care is the effective use of health information technology.

CHIME members take very seriously their responsibility to protect the privacy and security of patient data and devices networked to their systems. We appreciate the committee's interest in healthcare cybersecurity and the role that the Department of Health and Human Services plays in overseeing our rapidly progressing and innately innovative industry. We completely agree that cybersecurity must be a priority for HHS, just as it is for the nation's healthcare CIOs.

At Intermountain Healthcare, where the CISO reports to me, the CIO, we have made cybersecurity and privacy a major priority and focus. As an example, I have instructed my team that, as they prioritize their efforts each day, I would rather have our data centers go completely dark — meaning a complete loss of all of our information systems — than to have a major breach of our data. Losing our information systems would be horrible and highly disruptive, but our patients, members, employees, clinicians and others have entrusted us with their most personal data and we need to do all we can to protect it. Security is not an after-thought. Everyone across the organization needs to make it a priority. Even then, no system is perfectly secure.

To meet market pressures and regulatory requirements, including the Meaningful Use program and the shift to alternative payment models, CIOs have transformed their healthcare systems to become digital enterprises. This includes balancing the need to give clinicians immediate access to electronic protected health information while maintaining strict cybersecurity protocols. Some industries developed their information systems with a focus on security and restricted access (financial, government, security, etc.), however, in healthcare our systems were developed in a manner to facilitate rapid access to life saving data. This fundamental difference at the basic architecture and planned use of healthcare systems increases our challenge.

Further, there are several unique distinctions of the healthcare sector's data security environment that warrant consideration, including:

- Healthcare's highly-regulated environment
- The various settings where healthcare is delivered and data is required
- The range of resources available to devote to information technology and security
- Healthcare's unique financial models
- The frequency and volume of data exchange within healthcare delivery
- The increasingly mobile nature of healthcare technology and healthcare delivery
- Dependency on integration of systems and data (medical devices, niche applications, governmental requirements, business partners, etc.)

Cybersecurity in the Healthcare Industry

The Department of Homeland Security (DHS) deems healthcare one of the nation's 16 critical infrastructure sectors. The digitization of personal health information (PHI), the sharing of data encouraged and, in certain instances, required by the Meaningful Use program, and an increase in the "Internet of Things," has led to an increase in the number and types of cyber threats facing healthcare providers. For the second year in a row, criminal attacks were cited as the top cause of data breaches in the healthcare industry, with 50 percent of the breaches resulting from a criminal attack and 13 percent due to a malicious insider.[1] CIOs and CISOs face countless other malicious malware attacks on a daily basis, including Trojans, viruses, worms, and more. New threats will continue to arise, some can be anticipated while others will not, thus the notion of zero-day threats.

Meanwhile, providers with very limited resources, struggle to balance the huge demands for cybersecurity technology and information risk management programs. Threats to healthcare organizations are growing more sophisticated every day and too many health systems are not properly equipped to combat the myriad of attacks that could penetrate their networks. Even large healthcare delivery organizations that have made significant investments in security programs may fall victim to bad actors. We

[1] *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (Rep. No. 6). (2016, May 12). Retrieved May 12, 2016, from Ponemon Institute LLC website: http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1

have seen this with some of the largest retail organizations, financial institutions and even the federal government suffering large-scale breaches.

No industry can enable perfect security; rather organizations must enumerate and manage their risks. The healthcare organization and its IT security team are challenged with understanding every possible avenue of attack by which a hacker might gain access to the healthcare network, whereas the hacker only needs to find and exploit one weakness. In many cases, that one weakness is preying upon the behaviors of individuals through social engineering. As many studies have shown, and as many organizations that conduct penetration tests and other social engineering assessments will attest, it is impossible to prevent every human being in an organization from falling prey to such an attack.

Internal Coordination to Combat Cyber Threats

Given the breadth and depth of cyber threats, it’s paramount that all facets of a healthcare organization, from the information technology department to clinicians to the board of trustees and many in between coordinate efforts to improve the cyber hygiene of their organizations. While organizational and reporting structures vary by healthcare institution, coordination is imperative. The role of the healthcare CIO has evolved from being an IT director to an executive who is tightly engaged in nearly every facet of the enterprise. As such, CIOs have a holistic view of how various pieces of the health system are connected. That perspective is critical to providing a safe and secure environment, whether it is finances or clinical care.

As I mentioned earlier, at Intermountain, the CISO reports directly to me, the CIO. In our organization, the CISO is focused on developing and overseeing the implementation of the *technical strategy to achieve our security posture,* as well as managing our security team (Security Operations Center, Perimeter Services, etc.). Working across information systems (I.S.) operations ensures that the technical components required for cybersecurity are in place and managed. The interpretation of regulations, rules, corporate policy, procedure and *development of our security posture* (what we need to secure and how to set priorities) is the role of our compliance and privacy office, which reports to the board of directors. While these responsibilities are separate, our management structure helps us achieve a high-level of cooperation. My peer in Compliance and Privacy is aligned with me; the chief privacy officer is aligned with the CISO. Together we develop the plans and manage execution. We have developed a cooperative model for cybersecurity that insures appropriate checks and balances, but facilitates high levels of cooperation in achieving a more secure environment. This works at Intermountain. The focus isn’t on the CISO’s reporting structure. Rather, what’s important is that there is an appropriate focus and appropriate checks and balances on both security plan development and execution.

A similar structure is employed at Penn State Hershey Medical Center, Penn State Health System and Penn State College of Medicine, where the CISO reports to the CIO. The chosen structure was selected to build a strong cybersecurity program and transition to an IT shared services organization with tighter discipline, structure and process focus. This partnership ensures tight integration and solid support for the cybersecurity program across the entire IT team. Notably, the CISO established a "Cyber Security Advisory Council" that includes a number of key leaders from the organization. This group serves as the CISO's operational leadership link, offering input and direction independent of the CIO even with a formal CIO reporting relationship.

To exemplify the variation across healthcare delivery organizations, consider the following examples:

- At a large children's hospital, the CISO reports to the data security officer in order to combine expertise in data analysis and to take a more proactive approach to security. The CISO has dotted-line reporting to the chief compliance and privacy officer.
- The CISO at a large health system operating in two states reports directly to the CIO. The CISO is not only responsible for cybersecurity, but also account administration and disaster recovery.
- The CISO for a multi-state provider reports to the chief technology officer, who then reports to an enterprise-wide CIO.
- CHIME members at several smaller organizations report that they have the dual role of CIO and CISO.

Where the CISO should report is highly dependent on how the role is defined by the organization. As I stated, at Intermountain, the CISO is responsible for developing and overseeing the implementation of the *technical strategy to achieve our security posture,* managing our security team and working with I.S. peers to assure that the technical components required for cybersecurity are in place and managed. A different department acting as a check and balance is responsible for regulatory interpretation and development of the requirements for cybersecurity. This is not unlike other technology solutions where end users who own operational controls define requirements and I.S. handles implementation. Other organizations may choose to combine these roles. In such situations, different reporting relationships may make sense. I feel strongly, however, that there must be a continuous check and balance.

According to a March 2015 survey, 63 percent of AEHIS members indicated that they report to the CIO. Meanwhile, 16 percent report to the CEO and 11 percent report to the chief financial officer (CFO). According to a 2015 ThreatTrack study of 200 C-suite executives, the CISO reports to either the CIO or the CEO. The survey shows the prevailing trend is to put the CISO under the CIO, with 55.5 percent of respondents saying their CISO reports to the CIO, an increase of 10 percentage points from 2014. That compares with 40.5 percent who report to the CEO, a drop from 47 percent in 2014[2].

[2] *CISO Role Still in Flux: Despite Small Gains, CISOs Face an Uphill Battle in the C*-Suite (Rep.). (2015). Retrieved May 23, 2016, from ThreatTrack website: https://www.threattrack.com/getmedia/5d310c4c-aed6-4633-929f-0b5903d2bc79/ciso-role-still-in-flux.aspx

Further, CIOs may manage various pieces of the organization's IT infrastructure; some may manage biomedical devices, while others may not. Given the variability in reporting structures across the industry, federal policies must enable organizations to employ protocols that best match their IT security needs and the organization's internal IT workflow. Thus, it is important to emphasize it's not enough to rely on reporting structure changes to initiate meaningful change, instead security must be an organizational priority for true change to be enacted.

Cyber Readiness at HHS

In many ways, healthcare information technology is a maturing industry and HHS faces similar organizational challenges as today's healthcare CIOs. CHIME is pleased with the important advances set forth in the Cybersecurity Act of 2015[3] that was signed into law with the government funding package on December 28, 2015. Notably, HHS, by December 28, 2016, must present Congress with a report that identifies the individual who will be responsible for coordinating and leading efforts to combat cybersecurity threats. HHS must also present a plan from each relevant operating division with respect to how each division will address cybersecurity threats in the healthcare industry, and a delineation of how personnel within each division will communicate with each other regarding efforts to address such threats.

Just as healthcare institutions must coordinate efforts to thwart cyber threats, it is vital that HHS have a coordinated plan to address threats to the data and systems used and housed by the department. Further, the industry welcomes the direction Congress issued as it will mitigate some of the continued concern about contradictory or unclear guidance from different subdivisions of the department. Concerning the HHS Data Protection Act, CHIME suggests that such legislation account for the ongoing efforts within the agency to evaluate how best to coordinate efforts on cybersecurity.

Illustrating the need for improved coordination, CHIME members point to inconsistencies in the enforcement of the rules around the Health Insurance Portability and Accountability Act (HIPAA), the law governing privacy and security requirements providers must meet, as a major impediment to being able to implement sound risk mitigation strategies. The existing enforcement paradigm is heavily focused on compliance activities which in some cases actually make it harder for providers to commit resources to areas they deem to be worthy and critical. This can be a distraction or drain on already limited resources necessary to actually secure the numerous points of entry — medical devices, networks, EHRs. Variability around who is required to comply with HIPAA contributes to the difficultly providers face in securing each and every potential vulnerability.

HIPAA requires only three covered entities comply with the law: providers, payers, and healthcare clearinghouses. Business associates of these three entities must also commit to protecting PHI as part of their contractual relationships with covered entities. However, device manufacturers are not HIPAA covered entities. Our members often

[3] Consolidated Appropriations Act, 2016, 113 741 § Improving Cybersecurity in the Health Care Industry - 405 (2015).

describe scenarios in which medical devices are deployed with default passwords, some of which are unable to be changed by the providers. This creates a situation where once the device is connected to a provider's network it can be easily penetrated by bad actors, potentially threatening the functionality and safety of the device and introducing risk to the overall system. Worse than that, it creates a clear and present danger to the health and safety of the patients who have entrusted us with their care.

In other instances, today's current rules are insufficient to ensure interconnected devices adequately protect patients from harm and fend off privacy, cyber and other security threats. Additionally, some medical devices operate on private networks, not controlled by providers, creating large holes in perimeters and firewalls. CHIME recommended in recent comments to the Food and Drug Administration (FDA) that enhanced collaboration between device manufacturers and healthcare delivery organizations is necessary, and that the FDA approval of high-risk devices should include an assurance that the data collected and shared by the device is secure and that the device is not an easy entry point to a health system's network, as has been proven to be the case today.[4]

HHS Data Protection Act

CHIME encourages the committee to fully evaluate the potential negative consequences that could result from making the HHS CISO a presidential appointment. We've seen other instances where politicizing a role can hamper an agency's ability to affect change. For instance, Marilyn Tavenner in 2013 became the first Centers for Medicare and Medicaid Services administrator to win congressional approval since Mark McClellan, M.D., in 2004. That lack of official leadership creates uncertainty in the industry. Additionally, as a former member of the Health IT Policy Committee, a federal advisory committee created under Health Information Technology for Economic and Clinical Health Act (HITECH), I witnessed firsthand how important initiatives for improving care delivery can get bogged down in politics and bureaucracy.

As a healthcare CIO, I again echo the importance of coordination. What's central to this conversation is meaningful coordination, avoiding any unintended consequences of complex reporting that instead may impede the coordination and flow of information necessary to thwart cyber threats.

I would also ask the committee to consider these additional and essential actions to help the nation's healthcare providers improve their cyber readiness:

1. **Provide Ample Time to Ensure Cyber Readiness**. We are rapidly increasing the interconnectedness of the nation's healthcare system, and the Meaningful Use program, particularly what is proposed in Stage 3, will only accelerate information sharing with new sources using untested standards. Meaningful Use requires providers under Stage 3 to facilitate patient access to their records through application programming interfaces (APIs). As such, providers will be

[4] *Postmarket Management of Cybersecurity in Medical Device* [Letter sent April 21, 2016 to R. Califf, Commissioner, Food and Drug Administration]. Retrieved from https://chimecentral.org/wp-content/uploads/2014/11/CHIME-AEHIS-Letter-to-FDA-on-Device-Cyber.pdf

required to provide this access to applications chosen by patients. The rapid proliferation of new applications connecting to the system will create a host of new entrance points into providers' systems and cybersecurity vulnerabilities.

Rushing implementation of health IT raises patient safety and cybersecurity concerns. We believe it is premature to include such mandates in the Meaningful Use program given the lack of mature standards, especially relating to security. Therefore, CHIME suggests that Stage 3 start no sooner than 2019 to allow for additional time to ensure proper security protocols are in place before the widespread use of APIs is mandated.

2. **Incentivize security.** Budgetary constraints can severely hamper a hospital's ability to pursue sophisticated cybersecurity measures. As noted above, at some smaller organizations, the CIO also serves as the CISO and has few human and capital resources to allocate to security. In many cases, a hospitals total spend on health IT – everything from clinical IT systems to revenue cycle to data warehousing – only accounts for 3 to 5 percent of the total operating budget. Given the low degree of spending/resources for IT spending, policymakers should look for ways to encourage investment through positive incentives for those who demonstrate a minimum level of cyberattack readiness and mature information risk management programs. The federal government and the nation's largest retailers have found themselves victims of large-scale breaches, there's no question that healthcare providers are at a disadvantage especially as they transform to meet the demands of new payment models, many of which will lower hospital reimbursements. Can reimbursement schemes include cyber preparedness? Should MACRAs Clinical Practice Improvement activity list include security improvements? We believe so.

3. **Enabling the Use of a Healthcare-Specific Identification Solution.** Reducing the reliance on Social Security Numbers (SSNs) and other identifiable information that help bad actors execute fraud will immediately devalue health records on the black market. We need a healthcare identification solution that, if stolen, does not have the same potential for fraud and abuse. It is essential that Congress remove the language in the Labor-HHS Appropriations bill prohibiting HHS (in Sec. 510) from using any federal funds to "promulgate or adopt any final standard …. providing for the assignment of a unique health identifier for an individual." Technology has provided for alternatives to a numeric or alphanumeric identifier as a solution, and the government does not need to be the arbiter of the identification solution, but HHS must be able to provide technical assistance to private sector initiatives. Unfortunately, HHS has interpreted the annual funding ban to prohibit them from collaborating or assisting with private sector efforts to improve patient identification on a national level.

   As health information increasingly flows across unaffiliated providers in order to coordinate care and as patients increasingly access and share their own data, it becomes even more important to ensure that patients are accurately identified and matched to their data. Ensuring correct patient matched is the first step toward effectively protecting and securing identities and mitigating fraud. CHIME encourages subcommittee members to work with the relevant appropriations committees to loosen the annual funding ban and allow HHS to work with the private sector to improve patient safety by enhancing the ability of the health sector to accurately match patients to their data.

Recognizing that the industry can no longer wait, CHIME, through its Healthcare Innovation Trust, has launched a $1 million crowd-sourcing challenge to find a safe, private and secure approach to ensure accurate patient identification. The first phase of the competition saw 113 innovators from around the world submit ideas; more than 340 individuals and teams from 39 countries have registered for the National Patient ID Challenge. We expect to announce a final solution in February 2017.

4. **Reduce Regulatory Complexity**. Congress should pursue legislation that harmonizes other privacy, security and information risk management requirements to eliminate the complex patchwork of regulations across industries and state lines. Currently, healthcare organizations dedicate highly valuable resources to navigating these complexities to demonstrate compliance with its regulators; if a streamlined regulatory framework were in place these resources could focus more time on actively monitoring and protecting against the daily variable threats.

There is no question that the committee’s interest in this topic is timely, and efforts in the healthcare sector to improve the industry’s cyber hygiene must be met with similar efforts within HHS. On behalf of CHIME and my colleague healthcare CIOs, I sincerely thank the Committee for allowing me to speak to the ever evolving role of the healthcare CIO particularly as it relates to IT security. I look forward to answering your questions.