Subcommittee on Privacy, Confidentiality, and Security

Hearing on Security in Healthcare

Meeting Summary

July 14, 2021

National Committee on Vital and Health Statistics (NCVHS)

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

This report was written by NCVHS consultant Bethany Stokes, MS, and colleagues at Rose Li and Associates, Inc., in collaboration with NCVHS members and staff.

NCVHS Members and Staff in Attendance

Melissa M. Goldstein, JD,* ***Co-chair, PCS Subcommittee***
Jacki Monson, JD,* ***Co-chair, PCS Subcommittee***
Nicholas L. Coussoule, ***NCVHS Chair***
Tammy Banks, MBA
Denise Chrysler, JD*
Jamie Ferguson
Vickie M. Mays, PhD, MSPH*
Valerie Watzlaf, PhD, MPH*
Wu Xu, PhD

*Member of the Subcommittee on Privacy, Confidentiality, and Security

Staff

Rebecca Hines, MHS, Executive Secretary/DFO
Maya Bernstein, JD
Geneva Cashaw
Natalie Gonzalez, JD
Rachel Seeger, MA, MPA
Marietta Squire

See Appendix B and C for complete lists of meeting participants.

NCVHS—The National Committee on Vital and Health Statistics

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory [42 U.S.C.242(k)] public advisory body to the Secretary of the Department of Health and Human Services (HHS) in the areas of health data, standards, statistics, national health information policy, and the Health Insurance Portability and Accountability Act (HIPAA). In that capacity, the Committee provides advice and assistance to HHS and serves as a forum for interaction with relevant private sector groups on a range of health data issues. The Committee is composed of eighteen individuals from the private sector who have distinguished themselves in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services The HHS Secretary appoints 16 of the 18 committee members to 4-year terms. Two additional members are selected by Congress. The NCVHS website provides additional information at https://ncvhs.hhs.gov/.

Table of Contents

Note to Readers: NCVHS invited hearing participants to comment on this document, which reflects their review. The Subcommittee has included links to their written testimony in the text below. The transcript of their oral remarks made during the hearing may be found at: https://ncvhs.hhs.gov/wp-content/uploads/2021/08/Transcript-PCS-Hearing-July-14-2021-508.pdf. A recording of the hearing may be found at: https://ncvhs.hhs.gov/transcripts-minutes/recording-hearing-on-security-in-healthcare-july-14-2021.

Introduction and Overview

The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality, and Security (PCS) monitors major developments with regard to health information privacy and security. On July 14, 2021, the Subcommittee convened a meeting with health care industry stakeholders and cybersecurity experts to hear testimony focused on solutions for improving the security posture of the health care industry and the range of security challenges affecting the health care industry. Speakers provided presentations during four sessions: (1) health care security challenges, (2) State, Tribal, and other health care security perspectives, (3) emerging threats and preparedness across the health care industry, and (4) federal perspectives on security infrastructure and enterprise-wide risk. (See Appendix A for meeting agenda and Appendixes B and C for list of invited speakers and attendees). The meeting was structured to achieve three broad objectives:

- Understand current policies and practices involving data collection and use with respect to privacy and security during the COVID-19 Public Health Emergency.
- Understand challenges and potential areas of clarification in light of these practices, emerging technology developments, and new policy directions.
- Identify best practices and areas where additional technical assistance or guidance may be useful.

The Subcommittee seeks to translate the knowledge gained during this meeting into recommendations to the HHS Secretary regarding actions to improve health data safety and cybersecurity capabilities within the health care industry.

Addressing Health Care Security Challenges

Jane Wong and Sabrina Kidd, MD[1]

University of California, San Francisco (UCSF) Health and Sonoma Valley Hospital

Cyberattacks are a constant threat to any health care or university system. Recent attacks have targeted supply-chain systems (including SolarWinds and Accellion), and some have begun to target systems that accommodate remote workers, including Citrix or Pulse Secure VPN. Health care systems are now the third-most targeted industry, compared to the eighth most in 2019.

Sonoma Valley Hospital is a full-service acute care district hospital that provides medical care to the 42,000 residents of Sonoma, California. This hospital contains 24 acute care beds, with one hospitalist and emergency department physician on duty and numerous other specialists available on site. Sonoma Valley Hospital became affiliated with UCSF during 2018 and strengthened that affiliation in 2021 to include additional management service agreements for leadership positions, including a Director of Information Technology (IT) Services. The hospital is funded through revenues from services, parcel tax, charitable bequests, and donations for capital expenditures; the budget for IT services is approximately $3 million, which is only 5.2 percent of the total budget.

Sonoma Valley Hospital staff detected unusual network activities on October 11, 2020, and later identified a ransomware note, which led to notification of senior leadership and establishment of an incident command center. All computer systems were taken offline, and the downtime protocol was initiated; the hospital operated

[1] Ms. Wong and Ms. Kidd's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/1B-Wong-et-al-508.pdf

on paper for all procedures except mammography. Hospital staff engaged with cybersecurity experts, an external recovery team, and cyber attorneys. Investigations into the threat uncovered that the attack started through a phishing email sent to a user, and the threat actor then gained access to a privileged IT account that enabled access to other systems, causing encrypted imaging data to be extracted and backup data to be lost. Both clinical and administrative activities were impacted by the lost data. The recovery process took approximately 4 months and resulted in regulatory reporting to all government agencies, including the Office for Civil Rights (OCR) . Since the attack, Sonoma Valley Hospital with UCSF's help, improved internal IT processes, including periodic backup validation procedures, applying regular security patches, and a sustainable plan of software and hardware upgrade. Improved procedures also enabled multi-factor authentication and offsite backup and required regular password changes. In addition, 24-hour security monitoring was installed, and security training and education was provided to all hospital staff.

Community hospitals, such as Sonoma Valley Hospital, experience difficulties maintaining defenses against intelligence threats because their IT budgets and internal IT teams tend to be small. Fortunately, through its affiliation with UCSF, the hospital could access resources that were critical in recovering from the attack and building defenses to prevent future attacks from causing significant damage.

Erik Decker, MS[2]

Intermountain Healthcare

Intermountain Healthcare is a nonprofit health care system consisting of 25 hospitals, 225 clinics, a medical group with 2,600 physicians, and a health insurance company. Intermountain Healthcare leverages evidence-based best practices to consistently deliver high-quality outcomes at sustainable costs. The health care sector is part of 16 critical infrastructures identified by the U.S. Department of Homeland Security. The Health Sector Coordinating Council (HSCC), of which Mr. Decker is an Executive Council member, is the private sector–led advisory entity that was launched as a result of Presidential Directive 21 in 2015. HSCC represents small-, medium-, and large-size health care stakeholders that collaborate with government partners to identify and mitigate threats in vulnerability within the health care sector in order to deliver health care services to the public.

Health care systems have evolved to be better protected against cyberattacks, and, in turn, attackers have evolved in an attempt to overcome those safeguards. In 2021, the HHS Health Sector Cybersecurity Coordination Center(HC3) reported that 48 ransomware attacks impacted the health care sector, which is a significant increase from the prior year. In addition, approximately 72 percent of these attacks involved major data losses. In October 2020, the Cybersecurity and Infrastructure Security Agency (CISA), HHS, and the Federal Bureau of Investigation (FBI) produced a joint bulletin notifying the health care sector of threats of potential Ryuk ransomware attacks, some of which had already occurred and shut down multiple health care systems within a short timeframe. These threats were followed by the SolarWinds and Microsoft Exchange server cyberattacks. More recently, IT software management company Kesaya was impacted by a supply chain cyberattack that affected approximately 1,500 businesses in a single day. Each of these cyberattacks indicate that threat actors continue to innovate in order to cause more damage to the health care sector; thus, the health care sector must also innovate in order to stay ahead of threat actors and protect health care data. As a result of the Cybersecurity Act of 2015, HSCC and HHS created a 250-member working group called the HHS 405(d) Task Group, of which Mr. Decker serves as the industry co-lead, that developed the Health Industry Cybersecurity Practices (HICP) publication to provide the health care sector with best practices related to cybersecurity.

During July 2021, Congress passed Public Law 116-321, which recognizes that cyberattacks against health care systems are increasing and that the health care sector skews toward penalizing victims of cyberattacks. Under this new law, HHS will consider any preparatory cybersecurity practices undertaken by an organization over the past 12 months (in relation to a cyberattack) during its reviews of HIPAA-covered entities, thus incentivizing the adoption of cybersecurity methods. The law specifically addresses any work efforts promulgated under the HHS 405(d) Task Group as a 'recognized cybersecurity practice'. Because most cybersecurity programs are underfunded, Mr. Decker

[2] Mr. Decker's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/1A-Decker-Written-Testimony-only.pdf

proposes the development of a Center for Medicare & Medicaid Services (CMS)-based reimbursement model to fund cybersecurity programs, as well as the use of policies that continue to incentivize the development and upkeep of cybersecurity programs, rather than penalize them. Mr. Decker also emphasized the need to use publicly available best practices and guidelines, including the HICP publication and the many publications produced by the Health Care Industry Cybersecurity Task Force.

Within the Cybersecurity Act of 2015, health care organizations can share highly sensitive cybersecurity threat information with CISA and receive liability protections from regulatory enforcement; however, most organizations do not share such information because of concerns related to incident leakage and misinformation. CISA advocates for more intelligence sharing across the health care industry, including involved law enforcement agencies, which can help protect critical infrastructure. Mr. Decker recommends that the cybersecurity field develop an initiative to create improved bidirectional information-sharing between health care and law enforcement, share information from law enforcement to Information Sharing and Analysis Centers (ISACs), and provide education to critical infrastructures related to legal protections and sharing sensitive information with the federal government.

Denise Anderson, MBA[3]

Health Information Sharing and Analysis Center

ISACs are member-driven, trusted organizations that provide sector-related, all-hazards threat and mitigation information to other entities within a sector. Most ISACs have global members and operations, are not-for-profit entities that rely on membership dues for funding, and collaborate with the National Council of ISACs. The Heath-ISAC (H-ISAC) was founded in 2010 to offer health care stakeholders a trusted community and forum for sharing cyber threat intelligence best practices and mitigation strategies, as well as discussing recent threats and vulnerabilities. H-ISAC consists of representatives from many international health care–related organizations (e.g., biotechnology, pharmacy, health care system payers, and device manufacturing entities). The H-ISAC Threat Operations Center (TOC) includes a dedicated staff of security analysts that serves as an extension of the overall H-ISAC security team. In 2020, the H-ISAC TOC shared 77 threat information bulletins and 51 vulnerability information bulletins, received 798 victim notifications, and identified 185,413 member-shared indicators of compromise (IOCs).

Overall, H-ISAC plays a central role in sharing information on malicious sites, threat actors, threat indicators, malicious emails, software vulnerabilities, malicious software, risk-mitigation strategies, and incident responses with its members, government agencies, regulators, law enforcement, and global organizations. Most H-ISAC information is shared with members and partners through the H-ISAC Portal website, listservs, automated messaging, daily alerts and reports, weekly IOC reports, and monthly threat briefings. H-ISAC also hosts a podcast and regular webinars and has written white papers on data access management and strategic threat intelligence. H-ISAC convenes educational and networking events to facilitate collaboration among its working groups, committees, and members.

Not long ago, many health care systems were still reliant on paper record-keeping. Now, health care systems are dependent on electronic-based systems, which enable new, speedy methods of data transfer and collection. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 focused on promoting the adoption and meaningful use of health IT systems; however, the HITECH Act did not provide guidance related to cybersecurity. The evolution of technology and the realization of the value of health care data led to the paired evolution of threat actors that aim to gain access to a much larger threat surface. The number of ransomware-based attacks has nearly tripled since 2016, with many recent attacks targeting managed security service providers. In addition to ransomware, other attack types include insider threats, blended threats, social engineering, and phishing. Attacks can cause data exfiltration, intellectual property loss, data manipulation, data wiping, and loss of operational continuity; each of these effects can directly or indirectly impact patient safety and

[3] Ms. Anderson's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/1C-Anderson-July-14-2021-508.pdf

data integrity. Methods to prepare for such attacks include using enterprise risk management (ERM) approaches, maintaining an awareness of the threat landscape, and instating ecosystem training and information sharing.

Discussion

Cybersecurity Playbook

Ms. Wong recommended that HHS develop a cybersecurity-focused playbook that could be shared across the health care sector; this playbook would provide robust guidelines and solutions for a variety of cybersecurity issues and help organizations prevent and respond to attacks in a consistent manner across the industry. Participants agreed with this recommendation, adding that enhancing information-sharing across the health care sector would greatly improve organizations' ability to prepare for the most imminent types of threats.

Support for Cybersecurity

Mr. Decker recommended increasing support of risk management agencies operating through the Office of the Assistant Secretary for Preparedness and Response, which are typically understaffed. With more dedicated staff and resources, they could enhance cybersecurity preparedness, communication, and coordination.

Implementation of Public Law 116-231

Mr. Decker also recommended implementing Public Law 116-321 by submitting a Notice of Proposed Rulemaking—instead of a Request for Information (RFI)—in order to expedite the ability to implement this public law and help stakeholders understand how it can be used. Notices of Proposed Rulemaking enable sector stakeholders to provide comments and feedback on a given law and can help accelerate the implementation process more than an RFI process could.

Removal of Silos to Enable Communication

Participants emphasized the need to overcome silos within the health care industry in order to broadly and quickly share information related to cybersecurity. Some technical security silos are needed to safeguard specific patient data or information; however, in general, silos prevent rapid sharing of information that could be critical to preventing a cyberattack. In many cases, when an organization suffers a cyberattack, its lawyers limit communication to other organizations to prevent further data leakage; however, limiting communication may cause additional harm because real-time information could help prevent an attack at another organization. Many organizations do not share information because of fear of incurring regulatory consequences and thus a publication from OCR that details how communications can be performed would benefit the health care and cybersecurity fields as a whole.

Incentivization and Reimbursement Models

Mr. Decker emphasized that a value-based care model of reimbursement through CMS is the best method to incentivize organizations to engage in cybersecurity practices, instead of penalizing them for not participating appropriately.

Vendor Involvement

Participants expressed concerns related to vendor involvement during a cyberattack. Health care companies and institutions have converged on the same vendors for a variety of services, including Cloud-based storage of data or pharmaceutical manufacturing. Therefore, when one of these vendors is impacted by a cyberattack, multiple health care institutions can also be impacted. Thus, a vendor's ability to be prepared and respond to cyberattacks is critical and imperative to the functioning of the health care industry as a whole.

State, Tribal, and Other Perspectives on Healthcare Security

John Guerriero, MPP[4]

Senior Policy Analyst, Cybersecurity
National Governors Association

The National Governors Association (NGA) is the bipartisan organization of the United States' 55 governors that aims to address issues of national and state interest, share best practices and innovative solutions that improve state government, and support the principles of federalism. The NGA Center for Best Practices (NGA Center) hosts programs in multiple policy areas, including cybersecurity, public health, infrastructure, and education. The NGA Resource Center for State Cybersecurity, co-chaired by Arkansas Governor Asa Hutchinson and Louisiana Governor John Bel Edwards, provides governors with resources, tools, and recommendations to help craft and implement effective state cybersecurity policies and practices. Through the Resource Center for State Cybersecurity, the NGA Center offers states technical assistance and best practices in cybersecurity through a variety of vehicles. These include NGA Policy Academies, which are 1-year programs that support governor-appointed teams in developing strategic plans designed to address policy challenges, and a National Summit for State Cybersecurity, which NGA hosts annually to convene cybersecurity policy advisors and governor staff to exchange ideas and best practices. NGA hosts regular webinars to highlight emerging issues and successful state strategies related to cybersecurity and to provide a forum for peer-to-peer exchanges. NGA also helps states by providing technical assistance on request and producing publications about available policy options for addressing pressing cybersecurity issues.

The cybersecurity threat landscape is continuously evolving, and state and local governments are more vulnerable than ever before. This observation requires that state governments view cybersecurity as more than an IT issue, but as a whole-of-state issue, that must be addressed at the organizational and human levels. State cybersecurity risk management is not the sole responsibility of state IT departments – instead, the most robust frameworks bring all the resources states have to bear to address the issue, including the Governor's office, workforce and education systems and the state's homeland security apparatus as well as partners across industry, academia and federal and local government. NGA has identified five priority areas for state cybersecurity for which resources must be integrated to be prepared for a potential cybersecurity threat: cyber governance, critical infrastructure security, state and local partnerships, workforce development, and incident response planning. During the 2021 Cybersecurity Policy Academy on Advancing Whole-of-State Cybersecurity, Kansas and Missouri is focusing on cyber governance, Montana is focusing on workforce development, and Washington and Indiana are focusing on state and local partnerships. In previous Policy Academies, NGA worked with Indiana to draft and socialize a risk assessment tool,, Maryland to vet aspects of the state's security manual, Michigan to develop a state-wide cybersecurity framework for K-12 schools, Tennessee to develop strategic priorities related to cybersecurity for Governor Lee's Cybersecurity Advisory Council, Massachusetts to develop a cybersecurity toolkit for municipalities and develop plans for regional workshops to support municipal incident response planning, and assisted the Louisiana Cybersecurity Commission in crafting the Critical Infrastructure Cybersecurity portion of their statewide cybersecurity strategic plan.

Kevin Fu, PhD[5]

U.S. Food and Drug administration (FDA)

FDA has determined approximately 510,000 device submissions to be ineligible for approval based on cybersecurity concerns alone. The largest risk associated with medical device cybersecurity is not the potential of hacking into medical devices, but instead the unavailability of patient care and sensor integrity. FDA holds cybersecurity aspects of devices to a high standard because cybersecurity is akin to patient safety; thus, a medical

[44] Mr. Guerriero's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/2A-Guerriero-508.pdf
[5] Dr. Fu's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/4B-Fu-rev-July-14-2021-508.pdf

device is not safe for patients if it lacks proper cybersecurity safeguards. FDA has developed guidelines related to premarket and postmarket regulatory submissions and their cybersecurity requirements. The Content of Premarket Submissions for Management of Cybersecurity in Medical Devices guideline document details the engineering expectations related to cybersecurity during a medical device review; this document will be updated during 2021. The Postmarket Management of Cybersecurity in Medical Devices guideline document details how organizations can share information related to computer security vulnerabilities as they relate to medical devices.

In addition to submission guidelines, FDA has provided funding to the Medical Device Innovation Consortium and the MITRE Corporation to develop and host threat modeling bootcamps. Threat modeling focuses on identifying and analyzing risks to computer security using methods similar to hazard analyses; threat modeling best practices can be reviewed in the Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report 57. FDA recently submitted a response to the National Institute of Standards and Technology's (NIST) Request for Information related to critical software and threat modeling, and this report is available through the FDA website. FDA participated in the International Medical Device Regulators Forum and developed a manuscript detailing principles and practices for medical device cybersecurity, issues with legacy systems, and vulnerability management. FDA reviewed and endorsed the National Telecommunications & Information Administration's Software Bills of Material, which is a critical component of modern cybersecurity risk management. FDA also helped develop a Joint Security Plan (JSP), which is a total product lifecycle guide to developing, deploying, and supporting cyber secure technology solutions in the health care environment; the objective of the JSP is to establish a voluntary framework for medical devices and health care IT that enables sharing of cybersecurity practices, managing security risk of devices throughout the lifecycle of medical technology, and assessing maturity of a product cybersecurity program.

In 1975, the Institute of Electrical and Electronics Engineers (IEEE) released a publication detailing eight major engineering principles, two of which are highly relevant to cybersecurity. The open design principle states to not depend on ignorance of attackers or security by obscurity; this principle emphasizes that organizations should assume attackers know about and have access to all information in a given system and to build protections under that assumption. The second relevant principle is least privilege, which states that computer software should use the least amount of privileges necessary to complete a given function. If an attacker gains control over a given piece of software, one that has access to the least amount of privileges will produce the least amount of harm to the organization and thus the attacker is less likely to gain access to other realms of the server. Dr. Fu emphasized that more organizations should employ these two principles in their cybersecurity practices.

Dr. Fu outlined his five major priorities for 2021: (1) envision a strategic roadmap for future medical device cybersecurity, (2) integrate security principles via Center for Devices and Radiological Health (CDRH) guidelines, (3) train and mentor CDRH staff on premarket and postmarket device reviewing, (4) engage with stakeholders in medical device and cybersecurity ecosystems, and (5) foster cybersecurity collaborations across the federal government.

Discussion

Public Health Representation on Safety Review Board

Dr. Fu noted that President Biden's recent Executive Order to improve cybersecurity practices involves the creation of a new safety review board and recommended incorporating more public health representation on that board.

Legacy Systems

Mr. Guerriero recommended that HHS ensure that legacy systems are updated across organizations, possibly through increased funding, enhanced documentation, or guidance from an ISAC, in order to ensure that protection of those systems is maintained over time. Dr. Fu added that device procurement playbooks are available to help organizations procure and protect medical devices.

Cybersecurity Practices for Remote Working

Participants discussed the possible trends in cybersecurity attacks as many U.S. workers transition back to in-office work after working from home during the COVID-19 pandemic. Remote work increased many organizations' threat surfaces and therefore vulnerabilities; however, awareness of this issue has enabled many organizations to identify methods to increase protection for remote workers, which will benefit organizations that continue to permit remote work.

Preparedness for Small Health Care Systems

The COVID-19 pandemic highlighted that many small health care systems and hospitals are under-resourced, particularly in terms of cybersecurity capabilities. Participants emphasized that such systems should employ risk assessment tools to identify and mitigate possible vulnerabilities and to engage with ISACs and the H-ISAC to receive alerts that are relevant to all health care entities. Participants noted the need for increased communication and threat information sharing between health care systems and federal, state and local authorities.

Emerging Security Threats and Preparedness Across the Health Care Industry

Suzanne Widup, PhD, MS[6]

Verizon Enterprise Solutions

In 2021, Verizon Enterprise Solution released its 14th Data Breach Investigations Report (DBIR), which is a collection of cybersecurity-related information. The 2021 DBIR report contains information on 79,635 incidents and 5,258 data breaches that was provided by 83 contributors from 88 countries. Approximately 61 percent of the data breaches involved credential data, such as login and password information. In addition, approximately 10 percent of breaches involved ransomware, which is likely caused by enhanced technical methods that allow attackers to steal data during encryption; ransomware is now the third-most prevalent method used to cause data breaches. Cloud assets were more commonly targeted during data breaches than assets located in on-premises storage systems; this finding aligns with the noted decrease in attacks targeting specific devices (e.g., a staff member's computer) in favor of targeting more server-based databases. The 2021 DBIR found that most data breaches were executed by external and financially motivated actors and that the number of internal actor breaches, including accidental breaches, decreased. Verizon Enterprise Solutions also leverages data from the VERIS Community Database Project to monitor publicly disclosed breaches; data collected between November 2020 and July 2021 suggest that most breaches are caused by malware and hacking, followed by internal errors and misuse.

Since 2014, the DBIR has included cluster analyses of security incidents in order to efficiently identify patterns that inform understanding of the current state of data breaches and incidents. In the 2021 DBIR, the analyses identified that social engineering, web application attacks, system intrusion, and miscellaneous errors explain the methods used for most breaches. Web application and social engineering attacks have continuously increased in prevalence since 2016, whereas attacks caused by privilege misuse, lost or stolen assets, and denial of service have become less prevalent. Most web application attacks occur through hacking using stolen login credentials or brute force, and most of these attacks are now targeting the IT industry, followed by the previously most targeted industry, the financial industry. Approximately 95 percent of organizations that contributed to the DBIR incurred between 637 and 3 billion malicious login attempts throughout the year. Of the system intrusion-based attacks, greater than 70 percent of these attacks involved malware and 40 percent involved hacking; however, approximately 95 percent of ransomware attacks used system intrusion. Further, miscellaneous error-causing attacks were most likely to involve accidents caused by staff with the most access to privileged information, such as administrators, developers, end users, and security researchers. Despite decreasing, privilege misuse attacks continue to occur and are caused by abuse of privileges and malicious insider attacks; typically, greater than 30 percent of these attacks

[6] Dr. Widup's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/3A-Widup-508.pdf

take months, and sometimes years, to discover. Overall, most breaches in the health care system as a whole result from misdelivered information and publishing errors.

Kevin Stine[7]

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is a nonregulatory agency that aims to cultivate trust in technology by advancing cybersecurity and privacy standards, technology, and measurement science. NIST recently updated its foundational IT health care guide that focuses on educating readers about cybersecurity terms used in the HIPAA Security Rule—amplifying awareness of NIST and non-NIST cybersecurity resources relevant to HIPAA and providing information to support implementation for covered entities and business associates. NIST is now adjudicating comments received on the draft document and aims to publish the document soon.[8]

NIST's National Cybersecurity Center of Excellence (NCCoE) is a collaborative center that convenes expertise from industry, government, and academic institutions to address current and emerging cybersecurity issues. NCCoE has developed many publications that target specific cybersecurity topics, including methods to secure electronic health records (EHRs) on mobile devices and telehealth remote patient monitoring ecosystems. Some of these publications are also accompanied by tutorials. In addition, NCCoE also hosts workshops. One workshop was held to discuss improving protection against and responding to ransomware attacks, with the overall goal to develop a publication detailing standards and best practices in ransomware risk management. NCCoE is also updating a publication related to cyber supply chain risk management, which aims to help organizations manage the increasing risk of cyber supply chain compromise; this publication is planned for released in Spring 2022. NCCoE has developed a project to raise awareness of issues related to migrating resources to post-quantum algorithms and to develop practices that ease this migration and protect against quantum computer-based attacks.

NIST is also actively engaged with activities launched in response to Executive Order 14028, which seeks to improve the United States' cybersecurity capabilities; many of these activities revolve around publishing guidelines related to cybersecurity practices.[9]

Discussion

Threat Detection and Protection

Dr. Widup emphasized the importance of having methods of threat detection and testing those methods regularly to ensure that when an attack occurs, the system reliably notifies the organization's IT staff, who can then enact the appropriate protocols to prevent the threat from spreading or causing any damage. Mr. Stine agreed that threat identification is critical, particularly to instill resilience to threats; he added that in recent years, NIST has focused on providing additional resources to guide response and recovery capabilities, which were less commonly discussed than threat prevention and protection.

Telehealth Security

Telehealth increases patients' access to care, but poses new security risks and cybersecurity implications, each of which must be carefully evaluated by cybersecurity and IT staff.

---

[7] Mr. Stine's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/3B-Stine.pdf

[8] NIST's Call for Comments on SP 800-66 Rev. 2: Implementing the HIPAA Security Rule closed on July 9, 2021. SO 800-66 Rev. 2 had not been finalized at the time this Summary was published.

[9] Executive Order (EO) 14028, "Improving the Nation's Cybersecurity (14028)," was issued on May 12, 2021: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Additional DBIR Trends

Dr. Widup noted that the 2021 DBIR found that ransomware attacks involving stolen data intended to publicly shame a victim into paying a ransom have increased, as well as attacks involving attackers who threaten to release stolen data.

Amplification of Resources

Participants applauded the resources developed by NIST and other cybersecurity-focused organizations, noting that despite the importance of these guidelines, health care stakeholders may not be aware of them. Participants recommended proactively sharing diverse resources during meetings and conferences, including videos, infographics, and tutorials to spread vital cybersecurity practices.

Tailoring Cybersecurity to the Organization

Dr. Widup emphasized that approaches to cybersecurity are not one-size-fits-all. An organization must evaluate its risks and then tailor its approach to securing its data. Mr. Stine added that cybersecurity is not a problem to be solved, but a problem to be managed and the methods of risk management should be tailored to the organization's capabilities and needs.

Federal Perspectives on Security Infrastructure and Enterprise-wide Risk Management in Healthcare

Julie Chua[10]

HHS, Office of Information Security

Within the health care and public health sectors, most organizational staff are given access to more than 11 million files, with 1 in 10 sensitive files accessible to all employees and new employees immediately receiving access to more than 11,000 exposed files. Approximately two-thirds of organizations have more than 500 staff accounts with passwords that do not have expiration dates, and approximately 79 percent of organizations have more than 1,000 ghost user accounts enabled. Threats to the Healthcare and Public Health (HPH) Sector continue to increase each year and are growing in sophistication. In 2020, the average cost of a single data breach in the health care sector was $7.13 million, and organizations that neglect to comply with HIPAA rules and regulations can be fined up to $1.5 million. Ransomware-mediated attack attempts against the health care industry rose by 123 percent in 2020. Successful ransomware attacks cost the health care sector approximately $20.8 billion in downtime during 2020, double the amount incurred during 2019.

Cyberattacks within health care affect all aspects of an organization and thus must be viewed as an enterprise-wide issue. In particular, these attacks can severely impact patient safety. The health care industry requires sensitive information in order to ensure quality, continuity, and efficient delivery of care, and attacks can compromise each of these characteristics by erasing patient medical histories. ERM is an effective organization-wide approach to address the full spectrum of organizational risks and opportunities by considering the combined array of risks and opportunities as an interrelated portfolio, rather than addressing these within silos. As co-chair with NIST of the interagency Cyber-ERM Community of Interest, HHS co-lead the development of a Special Chapter on Integrating Cybersecurity. This chapter is included in the updated Federal ERM Playbook

HHS is designated as the HPH sector's Sector Risk Management Agency and is required to work with health care and public health institutions to strengthen cybersecurity risk management procedures including providing

[10] Ms. Chua's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/4A-Chua-July-14-2021-508.pdf

guidelines that aim to improve patient heath data security and privacy, as well as reduce the risk of disruptive cyber events that impact patient safety.

As part of its mandate from the Cybersecurity Act of 2015, Section 405(d), the mission of the HHS Office of Information Security's 405(d) program is to provide the health care and public health sector with useful and impactful resources, products, and tools that help raise awareness, as well as to share vetted cybersecurity practices that drive behavioral change and consistency in mitigating cybersecurity threats. This program's procedures and activities are driven by its Task Group, which consists of more than 230 information security officers, medical professionals, privacy experts, and industry leaders. Members of the Task Group actively collaborate on a host of resources including the cornerstone publication: "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," which outlines the top five threats facing the sector and the top? ten mitigating practices. The Task Group is also developing a cyber-ERM focused publication which aims to help organizations include cybersecurity in their overall risk management strategies. . In addition, the HHS 405(d) Program established a strategic marketing, communications, and engagement platform that encompasses cybersecurity informational webinars, bi-monthly cybersecurity newsletters, cybersecurity infographics and informative posters, timely cyber-event mitigation one-pagers, and a vast social media presence.

Timothy Noonan, JD[11]
HHS Office for Civil Rights

The Office for Civil Rights (OCR's) role in cybersecurity is to administer and enforce the HIPAA Security Rule through investigations, rulemaking, guidance, and outreach. There has been a substantial increase in the number of healthcare data breaches affecting 500 or more individuals (large breaches) reported to OCR (329 reported in 2016 increased to 648 reported in 2020). Presently, through June 2021, hacking is the most frequent (72%) type of reported large breach followed by those involving unauthorized access/disclosure (23%) and theft (3%). Additionally, there has been a substantial increase in ransomware as a cause of reported large breaches (36 reported in 2016 increased to 199 reported in 2020). Through June 2021, network servers (51%) and email (26%) are the most frequent locations of reported large breaches. This represents a significant increase from historical data showing that from September 2009 to December 2020, network servers and emails each accounted for 21% of reported large breaches.

OCR's 2016-2017 audit of HIPAA regulated entities found that most covered entities (86%) and business associates (83%) did not have a substantially compliant risk analysis and most covered entities (94%) and business associates (88%) did not have substantially compliant risk management in place. This is consistent with OCR's investigations, which frequently find evidence showing noncompliance with the HIPAA Security Rule risk analysis and risk management requirements.

Mr. Noonan discussed recent completed OCR investigations involving hacking, and identified common themes including the need for regulated entities to improve their cybersecurity defenses and HIPAA Security Rule compliance by fully integrating regular risk analyses and risk management in business processes; conducting consistent information system activity reviews (*e.g.,* regularly reviewing auditing logs, access reports, and security incident tracking reports); ensuring that access controls and authentication processes are in place; implementing audit controls that record and examine activity in IT systems; incorporating lessons learned from security incidents into overall security management; and providing training specific to an organization and job responsibilities in order to reinforce a staff member's role in protecting privacy and security.

OCR publishes a cybersecurity newsletter that features explanations of Security Rule standards and helpful best practices. Recent topics include controlling access to ePHI, HIPAA and IT Asset inventories, and Preventing, Mitigating and Responding to Ransomware. OCR and the Office of the National Coordinator (ONC) also developed

[11] Mr. Noonan's written testimony is available online: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/4C-Noonan-508.pdf

a Security Risk Assessment tool, which is designed to assist small- to medium-sized organizations in conducting security risk assessments required by the HIPAA Security Rule and CMS' EHR Incentive Program.

Discussion

Increasing Cybersecurity Compliance

Mr. Noonan noted that the healthcare industry must improve its HIPAA Security Rule compliance and its overall cybersecurity defense to better address the present and emerging threats to electronic protected health information. He added that a significant proportion of organizations fail to perform risk analyses or implement access controls, such as multi-factor authentication, which contributes to many avoidable breaches. OCR has increased its policy and enforcement staff to support increased investigations, guidance and outreach opportunities.

Cybersecurity Awareness through Education

Ms. Chua emphasized that more education for all organizational staff, not just IT professionals, will help enhance compliance and, more importantly, risk management practices. She added that the Office of Information Security encourages all stakeholders to educate its staff on the NIST framework of identification, protection, detection, response, and recovery in relation to cybersecurity. This universal framework can help stakeholder organizations identify gaps in their current cybersecurity protocols.

Third-Party Vendor Attacks

Recent cyberattacks on third-party vendors have exemplified the effect that these attacks can have on major health care systems and industries. Such attacks on covered entities can result in compliance reviews into all known business associates, as well as the covered entity itself. Business associates have contracts with many covered entities, which causes vendors to become more attractive targets to malicious actors. To combat these attacks, OCR has prioritized providing education on these threats and developing protections against ransomware and hacking.

Resource Curation

Ms. Chrysler noted that the abundance of resources related to cybersecurity may be overwhelming to a small- or medium-sized organization that is creating a new cybersecurity plan and suggested the development of a curated set of resources that provide the most critical principles and practices of cybersecurity (i.e., "Security 101").

Public Comments

No public comments were received.

Subcommittee Discussion

Recommendations for Cybersecurity Practices

Participants identified the following cybersecurity-related recommendations to provide to the Secretary:

- Foster health care sector–wide collaborations to rapidly share cybersecurity information
- Develop a cybersecurity playbook with easily implementable cybersecurity solutions and guidelines
- Engage in more counseling/incentivization strategies to encourage the adoption of cybersecurity practices, rather than relying solely on enforcement of requirements
- Help under-resourced health care systems hire more IT and cybersecurity staff
- Increase education and training regarding cybersecurity, including risk management practices

Participants emphasized the need for health care systems to reside in defense mode, not reactive mode, as well as the need to provide education and counseling to organizations about the importance and benefits of

robust cybersecurity practices. They noted that cybersecurity-related insurance costs have more than doubled in recent years; coupled with the fact that insurance cannot retrieve data records lost in a cyberattack, this fact indicates that insurance should not be viewed as sufficient protection against cyberattacks.

I hereby certify that, to the best of my knowledge, the foregoing summary of minutes is accurate and complete.

/s/ 10/28/2021

Nicholas Coussoule Date
Chair, NCVHS

Appendix A: Agenda

Wednesday, July 14, 2021

9:30 – 9:35 a.m. Welcome and Roll Call – Rebecca Hines, NCVHS Designated Federal Official

9:35 – 9:45 a.m. Opening Remarks – Melissa Goldstein and Jacki Monson, Co-Chairs, NCVHS PCS Subcommittee

9:45 – 10:00 a.m. Overview and Framing of Current Issues

10:00 – 11:30 a.m. Panel I – Addressing Healthcare Security Challenges – Jacki Monson (Moderator), NCVHS PCS Subcommittee Co-Chair, and Vice President of Privacy & Information Security Officer at Sutter Health

- Erik Decker, Assistant Vice President/Chief Information Security Officer, Intermountain Healthcare
- Jane Wong, Chief Information Officer, USCF Health and Sabrina Kidd, Chief Medical Officer, Sonoma Valley Hospital
- Denise Anderson, President, H-ISAC

11:30 – 12:00 p.m. Break

12:00 – 1:30 p.m. Panel II – State, Tribal, and other Perspectives on Healthcare Security – Denise Chrysler (Moderator), NCVHS PCS Subcommittee Member and Director, Mid-States Region, Network for Public Health Law

- John Guerriero, Cybersecurity Policy Analyst, Center for Best Practices, National Governors Association
- Kevin Fu, Acting Director of Medical Device Security, FDA

1:30 – 3:00 p.m. Panel III — Emerging Security Threats and Preparedness Across the Healthcare Industry – Nicholas L. Coussoule (Moderator), NCVHS Chair and Senior Vice President, Enterprise Business & Technology Solutions, Horizon Blue Cross Blue Shield of New Jersey

- Suzanne Widup, Senior Analyst, Verizon Enterprise Solutions
- Kevin Stine, Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory

3:00 – 3:15 p.m. Break

3:15 – 4:30 p.m. Panel IV — Federal Perspectives on Security Infrastructure and Enterprise-Wide Risk Management in Healthcare – Melissa Goldstein (Moderator), NCVHS PCS Subcommittee Co-Chair and Associate Professor, Department of

Health Policy and Management, Milken Institute School of Public Health, The George Washington University

- Julie Chua, Director, Governance, Risk Management, and Compliance Division, Office of Information Security and Government Co-Lead of the 405(d) Task Group

- Timothy Noonan, Deputy Director, Health Information Privacy Division, HHS Office for Civil Rights

4:30 – 4:45 p.m.	Public Comment
4:45 – 5:30 p.m.	Subcommittee Discussion: Review themes, identify potential recommendations and additional information needs
5:30 p.m.	Adjourn

Appendix B: Invited Speakers

Denise Anderson, President, H-ISAC

Julie Chua, Director, Governance, Risk Management, and Compliance Division, Office of Information Security and Government Co-Lead of the 405(d) Task

Erik Decker, Assistant Vice President/Chief Information Security Officer, Intermountain Healthcare

Kevin Fu, Acting Director of Medical Device Security, FDA

John Guerriero, Senior Policy Analyst, Cybersecurity, Center for Best Practices, National Governors Association

Sabrina Kidd, Chief Medical Officer, Sonoma Valley Hospital

Timothy Noonan, Deputy Director, Health Information Privacy Division, HHS Office for Civil Rights

Kevin Stine, Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory

Suzanne Widup, Senior Analyst, Verizon Enterprise Solutions

Jane Wong, Chief Information Officer, USCF Health

Appendix C: Public Attendees (by ZoomGov)

First Name	Last Name	Organization
Zina	Adams	New York State Bureau of Vital Records
Carl	Allen	Intermountain Healthcare
Denise	Anderson	H-ISAC
Michael	Cash	SoftwareOne, Inc.
Flavia	Chen	UCSF
Julie	Chua	HHS
Susan	Cochran	UCLA
C	Cowley	HHS-FDA
Krycia	Cowling	HHS ASPE
Rebecca	Coyle	AIRA
Kris	Decker	
Erik	Decker	
Lorraine	Doo	HHS-CMS
Michele	Dillon	Rose Li Associates
Evan	Dygert	Blue Cross Blue Shield Association
James	Dzierzanowski	Kaiser Permanente
Lobna	Elsherif	Ministry of health
Kevin	Fu	HHS-FDA
Alix	Goss	Imprado
Keith	Graat	
Violanda	Grigorescu	HHS
John	Guerriero	NGA
Nicholas	Heesters	HHS
John	Hennelly	Sonoma Valley Hospital
John	Houston	UPMC
Marc	Jastremski	HHS-CDC
Erum	Khan	UMBC
Sabrina	Kidd	Sonoma Valley Hospital
Sarah	Kitterman	Sutter Health
Krista	Kolls	
Susan	Langford	BlueCross BlueShield of Tennessee
Brian	Lee	CDC
Cassie	Leonard	Chime Central
Marilyn	Luke	AHIP
Jayne	Lytel	
Karen	Mandelbaum	Epstein Becker Green
Kristina	McCann	CoverMyMeds
Heather	McClane	
Heather	McPherson	Kaiser Permanente
Timothy	Noonan	HHS
Jon	Oliver	HHS
Amy	Purvis	Kaiser Permanente
Sarah	Radermacher	Optum
Terence	Rice	Merck & Co., Inc.

Linda	Sanches	HHS-OCR
Jody	Schweitzer	AIRA
Catherine	Sicker	Quadax
Stacie	Spiegel	HHS - OGC
Kevin	Stine	NIST
Bethany	Stokes	Writer, Rose Li Associates
Robert	Tennant	WEDI
Andrew	Tomlinson	Chime Central
Sue	Wang	NCCoE/MITRE
Suzanne	Widup	Verizon
Kim	Williams	Rose Li Associates
Jane	Wong	UCSF

Appendix D: List of Acronyms

CISA	Cybersecurity and Infrastructure Security Agency
CMS	Centers for Medicare & Medicaid Services
COVID-19	coronavirus disease 2019
DBIR	Data Breach Investigations Report
ERM	Enterprise Risk Management
FDA	U.S. Food and Drug Administration
HHS	U.S. Department of Health and Human Services
HICP	Health Industry Cybersecurity Practices
HIPAA	Health Insurance Portability and Accountability Act of 1996
H-ISAC	Health Information Sharing and Analysis Center
HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
HSCC	Health Sector Coordinating Council
IOC	indicator of compromise
ISAC	Information Sharing and Analysis Center
IT	information technology
JSP	Joint Security Plan
NCCoE	National Cybersecurity Center of Excellence
NCVHS	National Committee on Vital and Health Statistics
NGA	National Governors Association
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
OIS	Office of Information Security
PCS	Privacy, Confidentiality, and Security
UCSF	University of California, San Francisco