NCVHS Subcommittee on Privacy, Confidentiality & Security

Comments Received in Response to Request for Comment
Federal Register Notice: 86 FR 33320

Input on Solutions for Improving Security in Healthcare

Received as of July 14, 2021

	Organization	Signatory	Notes
1.	Intermountain Healthcare	Erik Decker Chief Information Security Officer	
2.	UnitedHealth Group	Mitchell W. Granberg Optum Chief Privacy Officer	

Testimony Before the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality and Security

Addressing Healthcare Security Challenges

July 14, 2021

[Oral testimony 15 minutes during 10-11:30 panel]

My name is Erik Decker, and I am the Chief Information Security Officer for Intermountain Healthcare. Intermountain Healthcare is a nonprofit system of 25 hospitals, 225 clinics, a Medical Group with 2,600 employed physicians and advanced practice clinicians, a health insurance company called SelectHealth, and other health services in Utah, Idaho, and Nevada. Intermountain is widely recognized as a leader in transforming healthcare by using evidence-based best practices to consistently deliver high-quality outcomes and sustainable costs. I am here today presenting on behalf of the Health Sector Coordinating Council (HSCC), where I serve as an elected member of the Executive Committee.

On behalf of the Health Sector Coordinating Council (HSCC), I thank the National Committee on Vital and Health Statistics' (NCVHS) Subcommittee on Privacy, Confidentiality and Security for inviting our input on improving the security posture of the healthcare industry and the challenges confronting our sector.

The healthcare sector is one of sixteen critical sectors identified by the U.S. Department of Homeland Security. The HSCC is a private sector-led critical infrastructure advisory council organized under PPD-21[1], representing large, medium and small health industry stakeholders working with government partners to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to our nation's citizens.

In summary, we have identified the following key areas of focus, which are described in greater detail below:

1. **Understanding the New Threat Landscape**: Threat actors continue to grow in sophistication while healthcare organizations struggle to maintain defenses
2. **Continued Incentivization:** Continue to innovate and support the nearly 1 million healthcare organizations to build cyber defenses
3. **Sector Response:** The healthcare sector has organized a strong response to these cyber threats
4. **Additional Policy Recommendations:** Additional measures to consider that can assist the healthcare sector

I. Understanding the New Threat Landscape

Historically the focus of threat actors has been related to theft and sale of sensitive data. As our sector has evolved to protect against these data concerns the threat actors have evolved as well. As noted by the HC3, in 2021 alone there have been a total of 48 ransom attacks against our sector[2]. Additionally,

[1] Presidential Policy Directive -- Critical Infrastructure Security and Resilience | whitehouse.gov (archives.gov)

[2] Ransomware Trends 2021

within the last year alone we are now seeing 72% of these ransom incidents including data leakage. Another study found a 55% jump in cyber incidents against our sector for 2020.[3] According to a joint bulletin authored by the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Health & Human Services (HHS), and the Federal Bureau of Investigation (FBI) last October, there was credible information of increased and imminent Ryuk ransomware threats to our sector. This was quickly followed by the SolarWinds Orion network management threat announced by CISA and then another related to Microsoft Exchange Servers. Just this last 4th of July a new supply chain attack, impacting the IT management software called Kaseya, has been reported to have caused impact to upwards of 1,500 businesses in one day[4]. If these attacks had occurred at the beginning of the pandemic, when the healthcare sector was reconfiguring its operations to support a response to the spread of the COVID19 infection, it could have caused catastrophic impacts on public health. This demonstrates threat actors continue to adjust and evolve to cause maximum impact to their victims.

The last several years have taught us that the threat actors will continue to innovate new ways they can cause damage and extort our sector. As we consider new innovative ways to protect our sector we must also consider how the threat actors will change in tactics, as they have in the past. Today we deal with issues of data theft, extortion and impacts to patient care due to our Health IT systems being unavailable. We must consider the ability of a threat actor to hold the integrity of our data for ransom as well. For example, it has been demonstrated through security research that malware can manipulate and inject realistic images of cancerous growth into MRI scans[5]. When radiologists looked at these images, 99% of them believed the scan had detected cancer. This kind of attack brings the "Deep Fake" to healthcare. A future attack could extort our ability to trust the very data that we use to treat and care for patients.

Cybersecurity incidents are not only a threat to national security, they are also a threat to patient safety, as attacks can cause denial of service, medical device corruption, and data manipulation that directly impacts clinical operations, patient care and public health. In addition, healthcare data and information remain lucrative targets for theft and exploitation, particularly through ransomware attacks and COVID-themed social engineering by criminal groups and adversarial nation states.[6] A series of recent bulletins testifies to these threats.[7]

II. Continued Incentivization

We are very pleased that Congress signed into law this past January, H.R. 7898[8] (now P.L. 116-321), which recognizes increasing and dire cyber threats against the health system, and that our regulatory structure under the Health Insurance Portability & Accountability Act (HIPAA) has skewed too heavily toward penalizing even the best prepared and well-resourced healthcare organizations victimized by cyber-attacks. The new law rebalances this inequity by directing HHS, when making determinations

---

[3] Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the U.S. Impacted - CPO Magazine

[4] Up to 1,500 businesses could be affected by a cyberattack carried out by a Russian group. - The New York Times (nytimes.com)

[5] Malware in CT/MRI machines can inject fake cancerous growths. (foglets.com)

[6] PowerPoint Presentation (hhs.gov)

[7] NCSC_China_Genomics_Fact_Sheet_2021.pdf (dni.gov), 20201222-001_FBI PIN.pdf (govdelivery.com)

[8] PUBL321.PS (congress.gov)

against HIPAA-covered entities and their business associates victimized by a cyberattack, to take into account the covered entity's use of recognized security best practices during the past twelve months. More importantly, this provision serves as a positive incentive for health providers to increase investment in cybersecurity for the benefit of regulatory compliance and, ultimately, patient safety.

Among the cybersecurity best practices recognized by this law are those established under Section 405(d) of the Cybersecurity Act of 2015. Section 405(d) was implemented as a joint standing task group of the HSCC Cybersecurity Working Group and HHS, composed of more than 250 volunteers from across the HSCC membership and HHS, of which I am the industry co-lead. The result, two years in the making, was a publication called "Healthcare Industry Cybersecurity Practices (HICP)", which provides scalable and voluntary cybersecurity principles and practices for use by providers of any size and ability. This publication is designed to be used across the sector, tailored to small, medium, and large sized organizations.

We are grateful for the support this new law will provide, but we are concerned that HHS has chosen to publish a request for information prior to the publication of a proposed rule. Adding an RFI to the comment process will inevitably slow the process and add another layer of bureaucracy that we cannot afford while cyber threats continue to advance, and healthcare providers try and keep up. As we know from the past year, many cyber-attacks have been successful and have brought some providers to their knees by forcing them to divert patients to other care settings and dropping down to paper records. These scenarios place patient lives in the balance and drive up the cost of care for the entire sector.

Per the U.S. Census Bureau, there are "907,426 businesses in the Health Care and Social Assistance sector[9]." Yet the majority of these businesses operate on very thin margins and consider cybersecurity to be non-revenue generating overhead costs. This means, practically, that the majority of these organizations underinvest in cybersecurity protections or rely on their IT department to absorb its obligations. Knowing that cyber safety is patient safety, this business paradigm needs assistance. Given that the Centers for Medicare & Medicaid Services (CMS) is the largest payer in the United States, I propose reimbursement models designed to directly fund cybersecurity programs be investigated. This revenue would help set a minimum floor of protection which is crucial for the public health and well-being as we embark in the digital age.

HSCC recommends NCVHS:

1. Advocate for the 405(d) HICP and other HSCC best practices which are freely available tools that can be used by the sector to strengthen individual and our collective cyber posture;
2. Request HHS move directly to proposed rulemaking for implementation of P.L 116-321 (HR 7898); and
3. Push for policies that incentivize, or reimburse, for healthcare providers who practice better cyber hygiene rather than punitive approaches that penalize them.

III. How Our Sector is Addressing Threats

A major component of the HSCC is its Cybersecurity Working Group, which represents more than 300 healthcare organizations, with over 600 members, in direct patient care, medical materials, health

[9] Health Care Still Largest U.S. Employer (census.gov)

information technology, health plans and payers, laboratories, biologics and pharmaceuticals, and public health. In the Cybersecurity Act of 2015, Section 405(c) directed the establishment of the Health Care Industry Cybersecurity (HCIC) Task Force. This HCIC Task Force produced a publication that outlined six imperatives and over 100 action items to combat this threat.

The HSCC Cybersecurity Working Group has organized around this HCIC Task Force Report and works in partnership with HHS to implement new publications and materials. The HSCC has made tangible progress toward recognizing and addressing numerous weaknesses in the cybersecurity of our systems, operations and supply chain, particularly through the formation of 15 Task Groups and creation of 11 industry-developed best practices and guidance developed (some jointly with HHS and FDA) over the past three years. These include resources on: medical device product security and management; cybersecurity practices for health delivery organizations based on the NIST Cybersecurity Framework (a mandate of §405(d) of the Cybersecurity Act of 2015); methods for tactically managing a cyber crisis; cybersecurity management of healthcare supply chains; telehealth cybersecurity; and protection of innovation capital such as vaccine research against cyber theft.

We encourage the continued partnership with our Sector Risk Management Agency (SRMA), HHS, as well as other key agencies within the federal government, such as CISA, the Federal Trade Commission (FTC), and law enforcement agencies such as the FBI.

IV. Additional Policy and Regulatory Imperatives

In addition to the HHS 405(d) Task Group's HICP best practices referenced above, there are several other areas which have the potential to help advance our sector's cyber posture if they can be adequately supported. We have described these below.

- **National Defense Authorization Act (NDAA)**: Section 9002 of the Fiscal Year 2021 National Defense Authorization Act changes the name of "Sector-specific Agency" as detailed in the Homeland Security Act of 2002, to "Sector Risk Management Agency" (SRMA). HHS is the SRMA for the Healthcare and Public Health Sector. Yet, HHS does not receive any direct funding to accomplish the responsibilities laid out in Section 9002 which includes, among many other things: reviewing the current framework for securing critical infrastructure, including: overseeing and regularly updating a cybersecurity risk framework for the sector; providing specialized sector-specific expertise to critical infrastructure owners and operators; supporting the sector overall through threat information sharing; and facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators.

- **Information Sharing**: The Cybersecurity Act of 2015 permits protected sharing of highly sensitive cybersecurity threat information specifically with CISA. This sharing provides liability protections from regulatory enforcement. Unfortunately, in the midst of a cybersecurity attack, most healthcare organizations will work directly with the respective law enforcement agency, such as the FBI or Secret Service, and limit further sharing due to concerns of incident leakage and misinformation. CISA has asked for more intelligence sharing from across the industry, yet in the midst of a crisis it's difficult to engage with all agencies in the manner they desire. It is recommended that the law enforcement agency serve as the funnel to CISA, sharing the threat intelligence information directly with CISA, in as near-real time as possible, so the government can help protect other critical infrastructure. Additionally, during a crisis, an organization quite often needs to have access to sensitive threat intelligence managed by law enforcement.

Unfortunately, law enforcement tends to be hesitant to share this information for fear of impacting their investigations. That same information is needed by the healthcare organization to assess its impacts and protect patient safety. Lastly, there continues to be ongoing misunderstanding among some providers around when threat sharing is allowed.

We recommend undertaking an initiative that; a) allows for improved bi-directional information sharing between healthcare and law enforcement; b) aggregates information sharing from law enforcement back into all the critical infrastructure Information Sharing Analysis Centers (ISACs); c) provide further education to critical infrastructure around the legal protections for sharing this sensitive information with the federal government; and d) more education on when threat sharing is permissible.

- **100-Day Plan** – Similar to the effort President Biden initiated[10] for the nation's electric power system against cyber-attacks, that involved a 100-day plan executed jointly by the U.S. Department of Energy, CISA, and the energy sector, we believe a like-minded effort aimed at the health sector would be highly beneficial. It would strengthen collaboration and resolve across the sector, especially in light of the pandemic we continue to fight. The energy plan involves soliciting feedback from their sector on how best to inform future recommendations for supply chain security in U.S. energy systems.

- **Support for HSCC** – Presently, our sector is run almost exclusively on volunteer donations. The two HSCC employees are funded by H-ISAC and all but one of our sector's workgroups are comprised largely by industry volunteers and some federal staff. Presently, the only workstream that has any HHS fulltime and contractor support is for the 405(d) HICP effort described above. The dedicated resources within HHS today support one Task Group, whereas the other 14 Task Groups are managed without dedicated support. The 405(d) workgroup, which produced HICP, is a shining example of what is possible with public-private collaboration. We recommend expanding the support outlined within the 405(d) program to the larger HSCC Cybersecurity Working Group.

- **Support for the SRMA** - As mentioned previously, the SRMA for the Health Sector is HHS. Within HHS, there are limited resources allocated to help coordinate between the various operation divisions (such as HC3, FDA, ONC, ASPR, OCIO) and ultimately with the sector. The result is most healthcare organizations are unaware of how to engage with HHS on these cyber related issues. We recommend providing further funding to ASPR, the HHS Operating Division tasked with engaging with the sector, to better coordinate and expand on the public-private partnership.

I appreciate the opportunity to present my perspective before this distinguished committee.

Erik Decker

Assistant Vice President & Chief Information Security Officer
Intermountain Healthcare
Elected Member of HSCC Cybersecurity Working Group Executive Committee
HHS 405(d) Industry Lead

[10] Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats | Department of Energy

UNITEDHEALTH GROUP

9900 Bren Road East, MN000-T000,
Minnetonka, MN 55343

July 13, 2021

Melissa M. Goldstein, JD
Associate Professor
Department of Health Policy and Management
Milken Institute School of Public Health
The George Washington University
950 New Hampshire Ave. NW, Second Floor
Washington, DC 20052

Jacki Monson, JD
Vice President
Privacy & Information Security Officer
Sutter Health
2200 River Plaza Drive
Sacramento, CA 95833

Re: National Committee on Vital and Health Statistics, Hearing of the Subcommittee on Privacy, Confidentiality and Security

Submitted Electronically: NCVHSmail@cdc.gov

Dear Ms. Goldstein and Ms. Monson:

UnitedHealth Group (UHG) is writing to provide comments to the National Committee on Vital and Health Statistics Subcommittee on Privacy, Confidentiality and Security regarding privacy and security protections for personally identifiable health information maintained by the health care community. UHG appreciates the deep responsibility of managing individually identifiable health information and serving as a trusted custodian of this information on behalf of the people we serve. It is our belief that individuals have the right to have their health information used responsibly and maintained securely by those entities that collect and share the information.

UnitedHealth Group is a mission-driven organization dedicated to helping people live healthier lives and helping our health care system work better for everyone through two distinct business platforms—UnitedHealthcare, our health benefits business, and Optum, our health services business. Our workforce of 325,000 people serves the health care needs of 142 million people worldwide, funding and arranging health care on behalf of individuals, employers, and the government. We not only serve as one of the nation's most progressive health care delivery organizations, we also serve people within many of the country's most respected employers, in Medicare serving nearly one in five seniors nationwide, and in Medicaid supporting underserved communities in 31 states and the District of Columbia.

The sharing of personal health information spans a range of emerging scenarios including "at-home" DNA and other health related testing, wearable devices such as smart watches, and third-party health applications that can be downloaded onto a mobile phone or tablet. These new uses and applications can promote better consumer engagement in their health care and improved decision making. Unfortunately, some businesses are not providing full transparency

to consumers regarding the use and sharing of their health care information and many entities collecting health information are not subject to state or federal privacy standards.[1]

The privacy and security of personal information is a growing national concern. A recent survey by the Pew Research Center indicates that 81% of respondents believe they have very little or no control over information about them collected by companies and 79% were very or somewhat concerned over how that information was used.[2] Other surveys show 65% of consumers stating that companies should take additional steps to protect their privacy[3] and 67% indicating the government should do more.[4]

Consumers have benefitted from longstanding state and federal privacy laws, such as the Health Information Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), which ensure health care organizations use data responsibly and protect the consumer from discrimination, misuse, or abuse. Consumers have an expectation of trust in institutions that access and use health care data. They should expect any entity using this data to act as a trusted custodian and to:

- Use health information solely for legitimate health care purposes (e.g., improving personal health, advancing health system performance, and new discovery);
- Observe all health care and other privacy and security laws and regulations;
- Protect health information at the highest standards;
- Advance data-driven solutions based on evidence, quality, and value;
- Offer a clear description of how health care information is used and protected;
- Ensure personal health information is not used for discriminatory purposes; and
- Maintain personal health care information correctly and responsibly.

UHG supports consumer choice and we encourage policies that empower individuals to make fully informed decisions about their health care services and products. A central component of this choice is trust and accountability in the entities that are collecting and using their health information. We ask your Subcommittee to consider the following as it examines the use and sharing of personal health information:

- The Department of Health and Human Services (HHS) should contribute as much as possible to U.S. Congressional deliberations about the need for a federal framework that regulates entities that are stewards of health information, but currently fall outside of HIPAA's statutory authority;

---

[1] For example, recent surveys of Direct-to-Consumer Genetic Testing Companies show lack of consumer transparency around how their information is used and shared. James W. Hazel and Christopher Slobogin, *Who Knows What, and When?: A survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies,* Vanderbilt Law Research Paper No. 18-18 (October 18, 2018) accessed at: Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies by James Hazel, Christopher Slobogin :: SSRN

[2] Pew Research Center, *Americans and Privacy, Confused, Concerned and Feeling Lack of Control Over Their Personal Health Information* (November 15, 2019) accessed at: Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information | Pew Research Center

[3] Harris Poll and Fin Partners, *The Societal ROI Index: A Measure for the Time We Find Ourselves In* (November 9, 2018) accessed at: Societal ROI Media Deck FINAL_FNL_High Res (theharrispoll.com)

[4] Deloitte, *2018 Global Mobile Consumer Survey: US Edition* accessed at: Five key accounting and tax challenges testing the sports industry (deloitte.com)

- HHS should work collaboratively with other federal authorities, such as the Federal Trade Commission, to develop high level health information privacy and security standards for business applications, not currently subject to HIPAA, to provide comparable requirements that align with HIPAA's protections;

- Federal agencies should create a certification process for the use of health information by these entities that provide minimum thresholds of privacy and security protections and promote transparency for how information is collected, used, and shared;

- HHS should develop standards allowing HIPAA-covered entities and business associate's additional flexibility to limit access to health care information by outside businesses—such as third-party applications—if they believe sharing the information would compromise consumer protections, including minimum privacy and security thresholds; and

- HHS should focus resources toward audit and monitoring activities (e.g., through its audit program, facilitated by seasoned professionals) of organizations that are stewards of health information but currently fall outside of HIPAA's statutory authority.

We appreciate the Subcommittee's focus on this important topic. Thank you for your thoughtful consideration of our comments. Should you have any questions, please do not hesitate to contact me.

Sincerely,

Mitchell W. Granberg
Optum Chief Privacy Officer
mitchell.granberg@optum.com