EXECUTIVES FOR HEALTH INNOVATION
ONE THOMAS CIRCLE, NW, SUITE 700
WASHINGTON, DC 20005
WWW.EHIDC.ORG
@EHEALTHDC

March 11, 2022

Ms. Dawn O'Connell
Assistant Secretary for Preparedness and Response
U.S. Department of Health & Human Services
200 Independence Ave, SW
Washington, DC 20201

Dear Assistant Secretary O'Connell:

Thank you for the opportunity to respond to the request for information (RFI) to help shape the 2023 – 2026 National Health Security Strategy. The healthcare and public health sector is considered a critical infrastructure sector. As such, it is essential that the industry maintain robust cybersecurity protections. While the majority of the industry is privately owned, the federal government plays an integral part in the cybersecurity efforts by coordinating efforts across industry partners, such as with the National Health Security Strategy. Below please find EHI's responses to the specific questions in the RFI.

What are the most critical national health security threats and public health and medical preparedness, response, and recovery challenges that warrant increased attention over the next five years?

Cyber-attacks and Ransomware:

It's not news that the number of cyber-attacks and ransomware has been on the rise. From 2019 to 2020, there has been an increase in cyber-attacks on all critical infrastructures.[1] Recent reports have found that, worldwide, there was an increase of 62%, and 158% in North America alone.[2] Breaches of healthcare data specifically has risen more than 55% in 2020.[3] The cost of cyber-attacks is also on the growing; the FBI believes that 2020 saw around $29.1 million demanded for ransom, which is more than 200% ($8.9 million) reported in 2019.

Cyber-attackers are generally driven by the pursuit of financial gain rather than a certain industry or company. While not all companies will pay the ransom, cyber criminals recognize that many will. Experts say that the rise in attacks is connected to companies' decision to pay the demanded ransom, in part due to the belief that it is the quickest, and cheapest, option.[4] Cybercriminals are driven to find the easiest targets that will result in the quickest and largest ransom paid.

[1] https://blog.sonicwall.com/en-us/2021/03/sonicwall-exposes-soaring-threats-historic-power-shifts-in-new-report/
[2] https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them
[3] https://www.securelink.com/blog/healthcare-data-new-prize-hackers/
[4] https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them

With this data in mind, hospitals and healthcare system are quickly becoming the largest target for cyber-attacks. There is no shortage of reasons for this being the case. For one, hospitals are seen as easy targets. Secondly, patient data and patient health records are worth more than any other piece of stolen data. These records have been found to go for approximately $250 on the dark web. Payment cards, considered the second most valuable, are sold for less than $6. [5]

While hospitals are the most lucrative hits, they can also be considered one of the more heinous. Hacking hospital systems and medical devices can quickly become lethal. When cyber criminals practically shut down the hospital, providers lack crucial information about their patients, medical staff cannot accurately care for patients, individuals receiving regular treatment, like chemotherapy, have appointments cancelled or transferred to another system, and ambulances having no choice but to reroute patients to other (possibly more distant) hospitals. [6]

The pandemic has only increased the threat to hospitals.[7] As the pandemic has strained hospital systems and staff, hackers and cyber criminals have increased their focus on these vulnerabilities. To hospital staff and leadership, it is becoming increasingly attractive to pay the ransom in order to get their systems unlocked, and more importantly continue to treat their patients.[8]

There are many preemptive steps hospitals can take before they are attacked. This includes updating policies around what specialist has access to specific data, building tools for system isolation in the form of network, or micro- segmentation, improved analysis of detected cyber events, and above all, up-to-date and comprehensive staff training for everyone. People are a critical last defense, and they should be trained accordingly. [9]

Cybersecurity and Digital Health Expansion:

Rapid telehealth expansion across the country can be seen as one of few silver linings to the COVID-19 public health emergency. Though telehealth was an appreciated form of patient care pre-pandemic, the public health emergency guided state and federal governments to re-evaluate the traditional form of patient care. The previously wide-spread barriers to virtual care were waived. These flexibilities were conducive to the wide and rapid expansion of telehealth, and this non-traditional form of healthcare became increasingly popular with patients, caregivers, and providers. Many believe that the rapid expansion of virtual care has led to unprecedented telehealth innovation.[10]

It's critical that this wide telehealth expansion be continued and build upon; the future of increased positive patient experience and access to quality healthcare depends on it. A Cleveland Clinic study released mid-2021, found that almost all patients interviewed (91%) believed that a virtual care visit made it easier to get the care they needed. 82% of those studied claimed that

[5] https://www.securelink.com/blog/healthcare-data-new-prize-hackers/
[6] https://www.boozallen.com/content/dam/home/docs/cyber/responding-to-ransomware.pdf
[7] https://www.paloaltonetworks.com/blog/2021/08/healthcare-organizations-are-the-top-target/
[8] https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals
[9] Ibid.
[10] https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

these virtual care visits were a good as an in-person visit.[11] With such obvious success, it would be devastating to many Americans who have come to rely on the access to high-quality healthcare and makes the importance of protecting patients and their data from bad actors utilizing a still strengthening platform even clearer.

Hospitals and healthcare systems, even before the pandemic, found it difficult to find a budgeting balance to ensure both outstanding security and patient care. With COVID-19 crippling even the most financially stable hospitals, finding the money to secure hospitals' IT systems and digital platforms with a budget already stretched too thin, can be a difficult feat.[12]

Hospitals and healthcare systems lack the funding to incorporate the necessary increase in IT specialists on their team.[13] Executives in the healthcare industry, reasonably, must put patient care before anything; though, it can be said that secure systems and confident data protections are just as critical to patient outcomes as new, state of the art devices. It's also understandably difficult decision. Plus, it should be noted that if IT specialists are doing their job well, the work is invisible to all hospital staff. It can easily be assumed that if everything, to the untrained eye, is going perfectly; it leads the financial decision makers to question why more money should invested in a department and system that looks to already working well.[14]

Increased awareness about the importance of securing the architecture of telehealth platforms and other digital medical devices is paramount. As mentioned before, good system and device security looks quiet to an outsider, but, often, it can be anything but. Almost half of hospitals studied in a recent study from CyberMDX and Philips have experienced an IT shutdown as a result of a cyber-attack, however just over 1 in 10 hospitals allegedly believe cybersecurity investment is a high priority.[15] The economic setbacks led to less of an ability to better defend themselves, and to evolve with the great technological advances barreling through the healthcare industry.[16] Executives in the healthcare industry need to be better informed before walking into the board room in order to ensure a full deliberation, with all the facts, is happening before finances are distributed.

What medium-term and long-term (i.e., over next five years) actions should be taken to mitigate these challenges at the federal government and/or state, local, tribal, and territorial level?

Notification of a Hospital Data Breach:

A recent report found that in 2021, on average, it took an average of 212 days to identify and confirm a breach and an average of 75 days to contain that breach. So, if an organization's system was breached on January 1st, and then took the total average of 287 days for the organization to both identify and contain the breach, the breach wouldn't be considered to have been contained until October 14th of the same year. [17]

[11] https://www.jmir.org/2021/6/e18488/
[12] https://www.kff.org/coronavirus-covid-19/issue-brief/funding-for-health-care-providers-during-the-pandemic-an-update/
[13] https://www.discovermagazine.com/technology/cyberattacks-on-health-care-are-rising-but-many-hospitals-arent-prepared
[14] Ibid.
[15] https://www.computerweekly.com/news/252505226/Hospitals-see-cyber-security-investment-as-a-low-priority
[16] https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals
[17] https://www.ibm.com/security/data-breach

The Cybersecurity Act of 2015 states that all covered organization must report a system breach to the federal government within 60 days of the breach's identification.[18] A lot can happen in 60 days and these influential decisions can affect patients, providers, caregivers, and will likely disrupt the local health ecosystem. With cyber criminals existing in the covered entity's system, sitting among confidential data and programs, the damage could be astronomical.[19]

There is currently legislation under consideration in Congress that would incentivize covered entities to report the breach as soon as possible, while also giving the Cybersecurity and Infrastructure Security Agency (CISA) the power of enforcement. The proposed legislation does vary on time for notification - some bills will require only 24 hours after discovery to report the breach[20] and others suggest 72 hours.[21] EHI encourages ASPR to continue to work with Congress and other federal partners to identify a time frame that is reasonable for the health system and also works to protect the industry.

What public health and medical preparedness, response, and recovery opportunities or promising practices should be capitalized on over the next five years?

Training Staff:

EHI believes staff training on cybersecurity should be a core component of the National Health Security Strategy. A 2021 study from Health ISAC found that only 50% of healthcare organizations are "training and informing users on an ongoing basis about security."[22] With technology innovating at a rapid pace, especially within the healthcare space, training that was appropriate a year ago is likely outdated and unhelpful. It's not only about base-level staff member being educated. The report finds that the least educated around security training and awareness are the senior executives; often the leaders of an organization, those in decision-making positions with expensive information are unaware of their role and responsibility. These senior executives have the final say in funding, but many lack the knowledge that IT and security are just as critical to patient care as a new medical device.

In the same theme, organizations should be training staff on their business relationships with third-party stakeholders. Healthcare systems and devices are become increasingly unsecure when staff are not trained regularly. It is crucial for patient safety and the security of all medical devices that all healthcare staff who work with third parties have a dependable understanding of their role in the assessment third-party stakeholders and have a knowledge of proper security practices.

[18] https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[19] https://www.ibm.com/security/data-breach
[20] https://www.congress.gov/bill/117th-congress/senate-bill/2407?s=1&r=47
[21] https://www.congress.gov/bill/117th-congress/senate-bill/2875/text
[22] https://h-isac.org/state-of-healthcare-security-and-privacy-whitepaper/

Cybersecurity Insurance and Hospitals and Health Systems:

As cyber-attacks increase substantially, and the physical and financial destruction escalates, hospitals, more than ever, are turning to cybersecurity insurance. In turn, as the demand for cybersecurity insurance rises, so do insurance costs.[23] A study of insurance brokers released by the Government Office of Accountability found that more than half of the respondents saw customer prices rise from 10% to 30% in 2020 alone. Only 15% of the respondents reported no increase in insurance prices.[24] As the attacks rise in frequency, the level of protection that insurance companies are providing as reduced. Hospitals are finding that they are paying more for considerably less coverage.

A 2022 Report from Gallagher Risk Management Services projects that cyber policy premiums will 100% to 300% higher than in previous years for those organizations who lack the "best-in-class" security controls in place. For large hospital, this can be a major roadblock towards cybersecurity protection. For small and rural hospitals, the option for coverage has become practically impossible. These hospitals, who face an even higher level of staff shortage, workforce burnout, and financial failure, cyberattacks are often substantially more damaging than similar attacks against larger hospitals. Small and rural hospitals stand little chance of securing similar levels of protection. [25]

Insurance companies have started to implement stricter guidelines necessary to be approved for coverage. These guidelines have slowly become more prevalent in the private cybersecurity healthcare community; what insurance companies demand for coverage has slowly become something similar to a wide regulation standard.[26] Without intervention, insurance companies will be driving the development of the cyber industry's security standards. EHI believes ASPR should work with federal partners to ensure addressing the skyrocketing costs and requirements of cybersecurity insurance.

<u>Conclusion</u>

Thank you for the opportunity to submit comments for the 2023-2026 National Health Security Strategy. We look forward to continuing to work with you and your colleagues on these important issues.

Sincerely,

Jennifer Covich Bordenick
Chief Executive Officer

[23] https://www.beckershospitalreview.com/cybersecurity/cybersecurity-insurance-costs-spike-up-to-30-amid-surges-in-ransomware-attacks-gao-report-finds.html
[24] https://www.gao.gov/products/gao-21-477
[25] https://www.healthcareitnews.com/news/rural-hospitals-are-more-vulnerable-cyberattacks-heres-how-they-can-protect-themselves
[26] https://campustechnology.com/Articles/2022/02/04/Cyberinsurance-Companies-Raising-Rates-Tightening-Requirements.aspx?Page=3