American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

Testimony

of the

American Hospital Association

for the

Subcommittee on Federal Spending Oversight and Emergency Management

of the

Committee on Homeland Security and Governmental Affairs

of the

U.S. Senate

December 2, 2020

Chairman Paul, Ranking Member Hassan and members of the Subcommittee, my name is John Riggi and I am the Senior Advisor for Cybersecurity and Risk at the American Hospital Association (AHA).

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the AHA thanks the Subcommittee for the opportunity to testify on, and your interest in, the important issue of cybersecurity threats faced by hospitals, health systems and the health care provider field. Now more than ever, we all realize how vital hospitals are to the nation's critical infrastructure and how important they are to our communities' health and safety.

Today, within the context of the COVID-19 pandemic, I will discuss increased incidences of cyber threats toward hospitals and health systems, the resulting, unique challenges confronting the health care sector, and what the federal government can and must do to help ensure appropriate mechanisms are in place to share threat information and defend the nation's hospitals and health systems from cyber attacks.

The AHA has a unique national perspective on these issues, stemming from communications with thousands of trusted hospital leaders across our field and robust interaction with federal agencies. We are privileged to serve as an effective platform to facilitate communication and cooperation between the government and health care in our common interest to defend the field and the nation against cyber attacks. We also welcome the opportunity to inform the work of this committee in this capacity and stand ready to assist as needed.

Hospitals and health systems appreciate the recent efforts by federal agencies such as the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Agency (CISA), Federal Bureau of Investigation (FBI), Department of Health and Human Services (HHS), National Security Agency (NSA) and United States Secret Service (USSS) to disseminate cyber threat intelligence and respond to cyber attacks targeting health care during this pandemic.

The most recent national threat advisory of imminent ransomware attacks targeting hospitals, issued on Oct. 28, 2020, by CISA, FBI and HHS[1], was a good example of timely and actionable intelligence being shared by the government in a coordinated effort across agencies.

THREATS TO HOSPITALS AND HEALTH SYSTEMS

Unfortunately, the aforementioned alert, CISA AA20-302A, is also a good example of the tremendously increased cyber risk faced by hospitals emanating from foreign cyber criminals and spies seeking to take advantage of hospitals that labor under the strain of caring for COVID-19 patients. The alert stated that "CISA, FBI, and HHS have credible information of an *increased and imminent cybercrime threat to U.S. hospitals and healthcare providers,"* which remain ongoing as of this date. This threat is very telling as to the nature of the cyber adversaries we face. The adversaries seek to exploit the global pandemic for financial gain, aware that ransomware attacks on hospitals disrupt patient care services and risk patient safety.

This ongoing threat is the most significant and widespread cyber threat to face hospitals since the global WannaCry ransomware attacks in 2017 perpetrated by the North Korean government.[2]

Hospitals, and the overall health care sector, have long been heavily targeted by cyber adversaries due to the various critical data sets in their possession that cyber criminals can easily monetize. Yet, during the pandemic, we have witnessed an increase in the frequency, severity and sophistication of cyber attacks on hospitals and health systems. The pandemic, therefore, has led to a cyber "triple threat" for hospitals and health

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[2] https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

systems: an expanded attack surface; increased cyber attacks of all types; and fewer available resources to bolster cybersecurity defenses.

Expanded "Attack Surface"

In preparation for and response to COVID-19, the health care sector rapidly deployed and expanded network- and internet-connected technologies and services to a scale never experienced in health care.

For example, technologies for telehealth, telemedicine, telework and cloud based services were quickly adopted and expanded due to clinical and operational necessity at the encouragement of federal and state governments. Many hospitals and health systems have also expanded, within care units, remote monitoring of ventilators and other medical devices. These actions were taken to improve efficiency and to preserve precious personal protective equipment (PPE) in departments whose focus is on caring for COVID-19 patients.

The expansion of network-connected technologies and health devices has resulted in an exponential expansion of network access points. For cyber criminals, this has translated into a greatly expanded "attack surface." In other words, there are now many more opportunities to exploit technical vulnerabilities and penetrate hospital networks. Telehealth has emerged as a lifeline for many patients during the pandemic and is one that must be sustained. Such patients rely on the access provided through telehealth; cybersecurity is, at its core, a necessary element of patient safety for hospitals and health systems.

Increased Cyber Attacks

Cyber adversaries have launched relentless attacks on hospitals and health systems. Hacking incidents of all types targeting hospitals and health systems increased significantly throughout 2020. According to data from the HHS Office of Civil Rights (OCR) Breach Portal on 11/27/20[3] for the three month period between Sept. 1 and Nov. 27 of this year, there were 162 active and resolved hacking incidents affecting 12.6 million individuals. Comparatively, there were 218 active and resolved hacking incidents for the eight-month period between Jan. 1 and Aug. 31, affecting 7.3 million individuals.

At the onset of the COVID-19 pandemic, there was a dramatic increase in phishing email campaigns directed toward the health care sector and the general public. Social engineering techniques, such as COVID-19-themed phishing emails containing malware and links to malicious sites, increased by nearly 700%[4] worldwide by some accounts. Such emails are sent under the guise of providing important COVID-19 information. They make fake promises; one example might offer for sale equipment made scarce by the public health emergency, such as N95 masks and lifesaving ventilators. Instead these emails are laden with malware and malicious links.

[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[4] https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

Phishing remains the primary method to introduce malware and ransomware into hospitals, requiring dedicated, diligent hospital staff to monitor and educate workforces that are already strained due to the pandemic. Phishing emails are used by criminals not only to launch cyber attacks, but to also perpetrate fraud and steal funds, again using COVID-19 as their entry point. For example, it is common for hospitals and health systems to receive emails promising to supply scarce PPE in exchange for a down payment; they later discover that the PPE was counterfeit and of inferior quality, or perhaps never existed.

Foreign-based cyber criminals have taken advantage of the pandemic to steal data and threaten patient care. According to U.S. government alerts, highly sophisticated foreign intelligence services and military units from China, Russia and Iran have launched cyber campaigns targeting health care to steal COVID-19-related research, such as treatment protocols and vaccine data. In a disturbing trend, hostile foreign intelligence services are working in conjunction with cyber criminals (whose hacking capabilities and access are most useful to them) to target a wide scope of networks, including those related to health care.

As evidence of this phenomena, on Sept. 16, 2020 the Department of Justice (DOJ) stated in regard to the indictment of two Iranian hackers, "Unfortunately, our cases demonstrate that at least four nations — Iran, China, Russia and North Korea — will allow criminal hackers to victimize individuals and companies from around the world, as long as these hackers will also work for that country's government…"[5] In another example from Sept. 16, DOJ stated that, "the Chinese government tolerated the defendants' criminal activity because those defendants were willing to work on behalf of the Chinese intelligence services."[6]

Data breaches through businesses associated with hospitals and health systems, including third-party vendors storing sensitive patient information, also continue to be a problem. According to the HHS Office of Civil Rights (OCR), this continues to be a significant factor in large data breaches impacting millions of patients.

Ransomware attacks are a considerable concern, especially for a hospital overloaded by caring for COVID-19 patients. Such an attack could interrupt patient care, or worse, shut down operations at the facility, thereby putting patient lives, and the community, at risk. This is what happened this past March 12 to Brno University Hospital in the Czech Republic. The hospital, which is among the Czech Republic's largest coronavirus testing centers, was forced to redirect patients to other hospitals. At the same time, another facility in the city of Brno, the Children's and Maternity Hospital, was also hit. There have been recent domestic examples of ransomware attacks on hospitals and health systems which result in the interruption patient-care services. Ransomware attacks on

[5] https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states

[6] https://www.justice.gov/opa/speech/remarks-deputy-attorney-general-jeffrey-rosen-announcement-charges-and-arrests-computer

hospitals can result in the cancelation of routine appointments and surgeries, delays in treatment, denied access to electronic medical records at critical moments – including drug allergy information – and the diversion of ambulances carrying trauma patients to emergency departments that may be further away.

Resource Constraints

The third threat hospitals and health systems are experiencing are the human, financial and technical cybersecurity resource constraints due to reduced hospital revenue. The AHA released a report in June which estimated total losses for the nation's hospitals and health systems to be at least $323.1 billion in 2020. Reduced revenue due to canceled elective surgeries and patients' reluctance to seek non-COVID-19-related medical treatment during the pandemic has significantly decreased hospitals' and health systems' financial resources, leaving limited funds available to enhance network defenses and to recruit and retain cybersecurity professionals. Hospitals' cybersecurity workforce issues are exacerbated by the fact that there is already a shortage of professionals capable of meeting the demand for cybersecurity talent across all industries and government; furthermore, the health care field often has more limited budgets for these personnel than other sectors of the economy.

In summary, hospitals and health systems face a perfect storm of factors leading to expanded cyber threats and risks– an expanded attack surface, increased frequency of cyber attacks of all types and constrained resources available to bolster cybersecurity defenses. Ultimately, the issues we are discussing today are key factors for patient safety and patient access.

EXPAND PUBLIC-PRIVATE PARTNERSHIPS AND CROSS-INDUSTRY EFFORTS

An increase in classified and unclassified threat information sharing through appropriate channels is an important step toward helping hospitals and health systems defend themselves. Although DHS, CISA, the FBI, HHS and the U.S. Secret Service have done a commendable job in sharing threat information with the health care field and producing timely and high quality joint intelligence products, more needs to be done.

Threat information must be coordinated among the various agencies, centralized, disseminated consistently and made available in both narrative and automated fashion. Further, it must be *free* – entirely absent of fees paid to any cyber threat information-sharing entity. It is especially important that technical indicators of compromise (IOCs), which are the lengthy and voluminous technical malware signature codes, be automated and made readily accessible to all trusted health care entities. This was the intent of the Cybersecurity Information Sharing Act of 2015.

Timely dissemination of threat intelligence in an automated fashion and other joint efforts can play an important role in derailing cyber attacks; it can also help organizations recover and resume operations more quickly in the event of an attack's

success. Both of those outcomes reduce the financial incentive for cyber criminals to carry out ransomware attacks.

The AHA, along with the Healthcare-Information Sharing and Analysis Center (H-ISAC), the Health Care Sector Coordinating Council (HSCC) and the HHS-sponsored Health Care Industry Cyber Security Task Force, has urged more public-private partnerships to improve cyber security in a “whole of nation” approach to defend against cyber threats.

In the realm of cyber defense there is no competitive advantage between organizations, especially in health care. All face the same threats and, thus, the same potential consequences. As a result, all have the same incentive to freely exchange threat information for the common defense as well as for the defense of public health and safety.

UNIQUE CHALLENGES FOR THE HEALTH CARE SECTOR

Health care is the only economic sector that possesses a combination of highly targeted data sets such as personally identifiable information, payment information, protected health information, business intelligence, intellectual property related to medical research and innovation – including genomic studies related to the development of precision medicine – and, as a critical infrastructure sector, national security information related to emergency preparedness and response in times of national crisis or war.

Each one of these data sets is heavily targeted by cyber adversaries. Individually, these data sets are highly valuable to the cyber adversary; together, they become exponentially valuable.

Also, health care records continue to command a premium price on the dark web because they have enduring value to cyber adversaries. In other words, unlike credit card numbers, one cannot cancel their blood type or a medical diagnosis. Stolen health care records may be the source of repeated health care fraud, used to fund more serious crime, including violent crimes by foreign gangs or be exploited on an ongoing basis for intelligence purposes by a nation-state.

VICTIMS OF CYBER ATTACKS SHOULD BE PROVIDED ASSISTANCE, NOT ASSIGNED BLAME

Despite complying with rules and implementing best practices, hospitals and health care providers will continue to be the targets of sophisticated attacks, some of which will inevitably succeed. The government often repeats the phrase, “It’s not a matter of if, but when,” in regard to an organization becoming a victim of a cyber attack. Organizations that are victims of breaches should be treated as victims of crime, an approach that has been codified in Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination.

Unfortunately, the federal government's approach toward victims of cyber attacks is sometimes inconsistent across agencies and often counterproductive.

For example, federal law enforcement agencies often request and *need* the cooperation of victims of breaches to further their investigations and disrupt the threat to the nation. Simultaneously, a hospital or health system may be the subject of an onerous and adversarial investigation by the HHS Office of Civil Rights; this can be disruptive and have a chilling effect in regard to the government's interest and efforts to obtain victims' cooperation with federal law enforcement.

The victims of attacks should be given support and resources; attackers are the ones who should be vigorously investigated and prosecuted. Even if an organization were the victim of a cyberattack, it does not mean that the organization itself was in any way at fault or unprepared. Similarly, a breach does not necessarily equate to a Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance failure. Instead, successful attacks should be fully investigated, and the lessons learned should be widely disseminated to prevent the success of similar attacks in the future. President Obama signed into law the Consolidated Appropriations Act, 2016, Public Law 114-113, which included the Cybersecurity Information Sharing Act of 2015 (CISA). Recognizing the seriousness of the cyber threat facing the nation and the private sector, Congress established through CISA a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators and defensive measures while protecting privacy and civil liberties.[7]

To encourage this sharing, CISA includes certain safe harbor protections from civil, regulatory and anti-trust liability for sharing conducted in accordance with CISA.

Since the passage of CISA, the cyber threats against health care and the nation have increased significantly. Every hospital and health system in America places utmost importance on protecting the security and privacy of the patient data. However, as the government publicly acknowledges, no organization is or can be completely immune from cyber attacks. Regardless of the amount of human, technical and financial resources devoted to cybersecurity by any organization, cyber risk to the organization can be mitigated, but never eliminated.

We recommend that, given the increased cyber threat environment and attacks specifically targeting hospitals and health systems, along with resource constraints imposed upon hospitals and health systems in response to COVID-19, *additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyber attacks*. We welcome the opportunity to explore this possibility with the committee.

DEFEND FORWARD

[7] https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability

A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; such attacks should therefore be aggressively pursued and prosecuted as such by the federal government. We use the term “prosecuted” in all senses of the definition related to the government’s capabilities and authorities, which include and extend beyond the government’s law enforcement authorities found under United States Code (USC) Title 18.

This situation is analogous to the attacks on our nation on Sept. 11, 2001. In the aftermath of those attacks, all of the government’s capabilities were brought to bear to detect, deter and disrupt terrorist organizations – including those operating outside of U.S. borders that were beyond the reach of the FBI. In its whole-of-government approach, the U.S. leveraged its military authorities under USC Title 10 and its intelligence authorities under USC Title 50 to protect the homeland from foreign threats operating from safe harbors provided by hostile nation states and non-cooperative foreign jurisdictions.

The laws typically used to prosecute cyber crimes are not commensurate with the level of harm cyber attacks on hospitals can cause. For example, USC Title 18 §1030 is the Computer Fraud and Abuse statute that is used to prosecute hacking activity and other crimes related to computers. It carries a maximum sentence of 20 years in prison. But, due to sentencing guidelines related to this statute, sentences meted out are often far less than 20 years. This is not a strong enough deterrent for an international ransomware criminal who could be reaping millions of dollars in illegal profits along with a low probability of being apprehended.

We do not need more laws to improve legal deterrence for cyber crimes against hospitals. Rather, we should make better use of the laws and other law enforcement tools that are already available.

For example, USC T18 §1030 is most appropriate for prosecuting some ransomware attacks, but can be made more powerful when combined with, or replaced with, alternate prosecution strategies, which include other federal statutes covering Racketeer Influence and Corrupt Organizations, money laundering, commercial extortion, homicide and even terrorism. These additional crimes carry far more serious penalties that are more consistent with the threat-to-life element presented by disruptive cyber attacks against hospitals.

The U.S. response to cyber attacks against health care infrastructure should expand beyond heavy reliance on USC Title 18 for criminal investigation and prosecution. The authorities provided under USC Titles 10, 31 and 50 should all be invoked as necessary to provide more effective and robust options to deter and disrupt foreign-based adversaries that attack U.S. hospitals and health systems.

Title 31 allows the Treasury Department, through the Office of Foreign Asset Control (OFAC), to put financial sanctions on foreign entities that have conducted or facilitated

cyber attacks against U.S. organizations. OFAC sanctions also make it a crime for any other entity or person to conduct business with an OFAC-designated entity.

Titles 10 (military authorities) and 50 (intelligence authorities) can improve domestic cyber defenses by putting the U.S. on the offensive. They could be invoked to take an "active" or "forward" defensive posture to proactively disable and disrupt foreign-based cyber threats. The vast resources, knowledge and capabilities of the U.S. Cyber Command, National Security Agency (NSA), CIA and the rest of the intelligence community are unmatched and could be used to augment and support law enforcement actions, in sequenced and coordinated operations as part of an overall national strategy, as was done in the during the war on terrorism in the aftermath of 9/11.

In October 2020, U.S. Cyber Command conducted offensive cyber operations aimed at disrupting the Trickbot botnet used to distribute ransomware[8] and the FBI indicted six Russian military intelligence officers[9] implicated in distributing destructive malware. This is an excellent example of a unified, coordinated government approach to the global cyber threat, utilizing a combination of elements of national power.

COORDINATED GOVERNMENT SUPPORT AND PARTNERSHIP ARE KEY TO STOPPING CYBER CRIME

Despite hospitals' concerted attempts to secure their cyber ecosystems, individual efforts to secure systems are insufficient to prevent all attacks. The Trump Administration has used executive orders to name 16 critical infrastructure sectors – including health care and public health – deemed essential to the security of the nation and directed federal agencies to prioritize securing federal systems. HHS is designated as the liaison for the health care sector. More broadly, the FBI has been designated as the lead authority on investigating cybercrime. Other agencies, including the Department of Homeland Security and the Secret Service, also play key roles in combatting cybercrime and providing guidance. Coordination across these federal resources is critical to ensuring the wide, effective and timely sharing of threat intelligence and defensive strategies. In addition, these agencies must be given the resources to not only respond to attacks, but also help vulnerable health care targets prevent attacks from occurring or succeeding.

We have seen that the most effective response by the government to aid health care victims of cyber attacks is a consistent unified approach in which DHS, FBI and HHS respond in a timely and coordinated manner*. A call to one should be "a call to all."* The National Cyber Investigative Joint Task Force (NCIJTF), which also encompasses intelligence community and Department of Defense assets, may be the platform to further refine and enhance inter-agency coordination and response efforts.

[8] https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html

[9] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

As referenced above, the CISA Act provided a mechanism for sharing information among private-sector and federal government entities and provides a safe harbor from certain liabilities related to that information sharing. Information sharing allows organizations to stay ahead of emerging cybersecurity risks and contribute to our collective knowledge of threats. However, the goals of information sharing have yet to be fully realized. Expedited, tailored and automated cyber threat information sharing on a regular cadence from the federal government would benefit all health care and public health organizations. Providers need actionable information that identifies specific steps they can take to secure against new threats. Large volumes of more generalized information can prove challenging to interpret and may even become a distraction.

HHS also is directed under the Cybersecurity Information Sharing Act to work with the private sector and other federal agencies to establish voluntary, consensus-based best practices. While the federal government is working to provide additional educational and other resources to the health care field, more action is needed to address the cybersecurity challenges facing all sectors. As a nation, we must bolster the security of our cyber ecosystem, not just place the burden on individual institutions. Indeed, the magnitude of the challenges and the growing sophistication of the attacks suggest that the federal government must provide additional nationwide resources. These include efforts to:

- develop and disseminate coordinated national defensive measures, including leveraging national technical defenses which are used to protect government agencies;
- strengthen and expand our cybersecurity workforce through grant programs and retraining efforts, perhaps with a particular focus on the retraining of veterans;
- identify and disrupt bad actors;
- increase the consequences for those who commit attacks; and
- identify and support best practices by the private sector.

CONCLUSION

Hospitals and health systems, and the patients they care for every day, are heavily targeted by cyber adversaries, including sophisticated nation-states. They have made great strides to defend their networks, secure patient data, preserve health care services' efficient delivery and, most importantly, protect patient safety. However, our field cannot do it alone. Hospitals and health systems need more active support from the government to defend patients from cyber threats.

Conversely, the federal government cannot protect our nation from cyber criminals alone either – they need the expertise and exchange of cyber threat information from the field to effectively combat cyber threats.

What is truly needed is close cooperation between the government, the health care sector and all critical infrastructure via a formal exchange of cyber threat information and combined cyber defenses – truly a "Whole of Nation Approach."