“Defending Forward” in Healthcare: Supplementing Cyber Strategy

Emile Shehada, YLS ‘22

Hospital cybersecurity has become more relevant than ever to a meaningful national cybersecurity strategy in light of the ongoing public health crisis presented by COVID-19. Hospitals are especially vulnerable during public health crises; their already-urgent work becomes even more sensitive to disruptions, such as ransomware attacks. Hospital administrators are aware of their exposure to attacks and warn that the attacks that have already occurred are just the beginning. Ill-equipped to close or otherwise remedy cybersecurity breaches, hospitals are often forced to pay ransom demands—as in the case of Hollywood Presbyterian Hospital in 2016 and, more recently, Champaign-Urbana Public Health District in April 2020—or otherwise simply write off their losses. Social distancing and quarantine measures prompted by COVID-19 have shifted much national activity online, including many hospital operations. If the cybersecurity capabilities of hospitals were taxed before by their ordinary day-to-day activities, it is no stretch to imagine that the present crisis has pushed them to their breaking point.

Hospitals themselves certainly seem to believe that they are in different cybersecurity circumstances than before the current pandemic. The number of ransomware attacks on hospitals is on the rise, and hospitals have less time to work around them when they happen. In 2016, when COVID-19 was mercifully unknown, Hollywood Presbyterian paid $17,000 in ransom to unlock its systems and regain access to patient data. This past April, Champaign-Urbana Public Health District paid more than $300,000 to recover data after a similar ransomware attack, citing the time pressure imposed on it by COVID-19. More broadly, the interest groups and professional associations representing doctors and hospitals have been collaborating to create and disseminate cybersecurity best practices to their members. For instance, in April 2020, the American Medical Association and the American Hospital Association released cybersecurity guidance to doctors handling protected health information (PHI) from home. The focus on cybersecurity during the COVID-19 crisis contrasts sharply with the comparative irrelevance of the issue during the 2009 H1N1 pandemic and the 2014-16 Ebola outbreak.

Given that hospitals themselves are signaling the particular importance of cybersecurity during the ongoing crisis, it is incumbent upon the Department of Defense (DOD) and other relevant government stakeholders to consider how to implement DOD’s “defend forward” cyber strategy with respect to the healthcare space.

Making “Defend Forward” Relevant to Hospitals

“Defend forward” was inaugurated in 2018 in the DOD’s Cyber Strategy and an accompanying White House National Cyber Strategy document. Much time and effort has been devoted to explicating the idea of “defending forward.” Suffice it to say that “defending forward” is about proactively confronting and disrupting adversaries—primarily other nation-states—before they can execute attacks against U.S. networks. For example, “defending forward" might involve preemptively hacking an adversary nation-state's offensive cyber experts to keep them from carrying out their plans.

Unfortunately, there is some extent to which this definition of "defend forward" does not provide a cognizable solution to hospital cybersecurity vulnerabilities. Perhaps "defending forward" has stopped some nation-state adversary from directly attacking U.S. hospitals. Insofar as this has actually taken place, however, it is unlikely we will ever know. To the extent that it focuses on threats from nation states, however, it offers hospitals no protection from the more mundane—yet likely more germane—threat of cybercriminals. Cybercriminals have demonstrated that they are willing to attack during public health crises, and their attacks are more than capable of endangering patient safety. Hospital systems that fall prey to ransomware attacks are just as vulnerable to outright vandalism. Hospitals that fail to pay their ransoms often lose not just crucial medical records but the underlying hardware as well. That these attacks are not perpetrated by nation-state adversaries is likely small comfort to the hospital administrators who must, in any event, scramble to either raise the ransom or locate replacement equipment without endangering patients.

This is not to say that "defend forward" has nothing to offer the healthcare sector. In early April, the Australian Signals Directorate (ASD) used its offensive cyber capabilities to disrupt cybercriminals exploiting the COVID-19 crisis. This undoubtedly relieved some of the pressure on Australian hospitals. The ASD's offensive actions are only half the story, though; since the start of the crisis, it has been working with major tech companies, as well as Australian telecommunications providers, to harden the country's systems against attack. What this suggests is that "defend forward" may be profitably viewed as twofold. That is, it could encompass not just explicitly offensive tactics, but also defensive tactics that enable the offensive tactics to be more effectively and rapidly brought to bear. In the context of healthcare, "defending forward" in this manner would offer hospitals comprehensive protection from both nation-states and cybercriminals.

Accordingly, in order to be relevant to the threats that face hospitals, DOD's "defend forward" would need to be expanded to include active target-hardening. That would require the government to take steps to ensure that hospitals meet minimum national cybersecurity standards. This might include anything from setting an explicit cybersecurity standard independent of HIPAA to budgeting for federal cybersecurity aid to creating a statutory cause of action against hospitals that fail to adequately secure PHI.

Cybersecurity Challenges in Hospitals

The absence of a minimum hospital cybersecurity standard is a major cause of the frequency with which hospitals are successfully attacked. Cybersecurity corporations have repeatedly noted that hospitals, physicians, and medical equipment manufacturers alike fail to abide by or enforce even the most basic cybersecurity best practices. For example, FireEye's 2020 report on hospital cybersecurity observes that hospitals routinely fail to implement multi-factor authentication (MFA). MFA has become a staple at many corporations and universities and is frequently deployed at scale, including in hospitals. Yet a 2015 report by the U.S. Office of the National Coordinator for Health Information Technology (ONC) discovered that as of 2014, less than 50 percent of U.S. hospitals had the infrastructure in place to use MFA. The ONC report did not identify what proportion of U.S. hospitals actually used MFA, and ONC has not released a follow-up report. Given the growth of the healthcare MFA market, it is certain that more hospitals are actually implementing MFA. Nevertheless, a 2019 report by LastPass suggests that only 26 percent of healthcare enterprises use MFA, corroborating the observations in the FireEye report.

Similarly, hospitals and medical equipment manufacturers also do not consistently or effectively enforce encrypted connections between devices on the hospital's network. In a 2019 study, researchers at Israel's Ben-Gurion University announced that they were capable of adding or removing evidence of medical conditions in CT and MRI scans. The researchers trained a generative adversarial network (GAN, a machine learning model) to "inject" tumors into CT scans of clean lungs and to "remove" tumors from CT scans of cancerous lungs. Then, with the permission of the host hospital, they demonstrated that they were able to orchestrate a man-in-the-middle (MITM) attack on the link between the CT machine and the cloud database to which the machine uploaded the scans. Their loudly-trumpeted findings prompted at least one academic report to conclude that machine learning would be the next major threat to hospital cybersecurity. This was, of course, a dramatic overstatement. A cursory examination of the details of the attack reveals that the MITM attack was successful simply because neither the hospital nor the manufacturer of the CT machine had provided any means to encrypt the connection between the machine and hospital systems. The cybersecurity researchers' GAN was altering information that had been sent as cleartext—information that included the username and password of the physician or specialist making the scan.

On the one hand, it is a relief to know that we do not yet have to fear cybercriminals breaching patient privacy with the aid of machine learning techniques. On the other hand, it is disturbing to know that not only sensitive health information but also physician user credentials may be routinely transmitted without any form of protection from even the simplest MITM attack. Nor is there any reason to believe that this was an exception. A 2018 Infoblox survey revealed that only around 50 percent of U.S. hospitals are investing in comprehensive encryption for PHI communicated on their networks. It is difficult to imagine simpler cybersecurity measures than MFA and encryption—and yet well over half of U.S. hospitals may not use these measures.

These cybersecurity failures are symptomatic of a systemic underappreciation of the importance of cybersecurity. This may stem in part from hospital administrators conflating HIPAA cybersecurity compliance with genuine cybersecurity best practices. Although doing so is plainly misguided, it is not impossible to understand why they might make that mistake. Robert Kaplan of Harvard Business School and Anette Mikes of Said Business School write that organizations tend to treat risks as mere compliance issues when they have insufficient expertise with those risks. There is no reason to believe that hospitals would have any *a priori* expertise with cybersecurity that would help them preemptively formulate a robust cybersecurity policy. That said, HIPAA compliance is no substitute for a best-practices cybersecurity policy. HIPAA is largely static; the HIPAA cybersecurity standards do not and cannot evolve to adapt to new cybersecurity threats. Additionally, HIPAA is enforced by the HHS Office for Civil Rights (OCR), whose primary power is to conduct intrusive breach investigations and punitive compliance audits. To be sure, this power is a valuable "stick" against hospitals that might otherwise disregard their cybersecurity obligations. But OCR lacks any meaningful proactive advisory powers that could help it nudge or guide hospitals into compliance, and in any event often declines to take enforcement actions. Consider OCR's record on enforcement of HIPAA's Security Rule. The rule requires covered entities to report PHI breaches to HHS without unreasonable delay within 60 days if 500 or more individuals are affected, and within 60 days of the end of the calendar year otherwise. However, a 2019 report by cybersecurity consulting firm CynergisTek indicates that 2018 HIPAA Security Rule compliance among covered entities was only around 72 percent—and even that was a decline of two percent from 2017. Even so, OCR did not enforce the rule at all until 2017, and in 2019 only enforced the rule ten times.

Moreover, even outside the context of HIPAA, there has been little federal leadership on healthcare cybersecurity policy. When Congress passed the Cybersecurity Information Sharing Act of 2015, it specifically called for the Secretary of HHS to support voluntary efforts to improve cybersecurity provided such efforts are consistent with HIPAA. This may have sent a message to hospital administrators that efforts beyond HIPAA—that is, *in*consistent with it—were not a federal priority. DOD's "defend forward" strategy document and its White House counterpart make no mention of security for healthcare or hospitals. It is thus somewhat unsurprising that hospitals have failed to achieve some kind of industry-wide cybersecurity best practices independent of HIPAA.

Perhaps falsely buoyed by achieving HIPAA compliance, hospitals tend not to invest adequate resources in defining and implementing effective cybersecurity policies. MalwareBytes' 2019 report on hospital cybersecurity discerns that hospitals often fail to appropriately budget for cybersecurity because it does not generate revenue for the organization. Budget compromises usually force hospital IT teams—as well as the hospital more generally—to rely on outdated, unsupported legacy systems. According to the Healthcare Information and Management Systems Society's 2019 report, as much as 69 percent of healthcare organizations have at least some legacy systems left in place. 15 percent of healthcare organizations have more than 10 percent legacy systems remaining, while another 13 percent were unable to identify the number of legacy systems remaining. Of these respondents, 48 percent said their systems were still running outdated versions of Windows Server, and a staggering 35 percent reported that they were still running Windows XP. Given that healthcare providers tend to be unaware of 25 to 40 percent of the devices on their networks, these numbers might actually be higher.

These legacy systems indisputably jeopardize PHI. Even in the absence of malicious behavior, legacy systems can lead to accidental cybersecurity breaches. For example, in September 2019, the Vancouver Coastal Health Privacy Office disclosed in a press release that it had been inadvertently broadcasting PHI over its near-obsolete paging system. This PHI included patient names, ages, diagnoses, room numbers, and medical record numbers. When malicious behavior *is* involved, though, legacy systems expose their institutions to much greater harm. WannaCry and NotPetya, arguably the two most infamous pieces of malware from the past five years, exploited a vulnerability in legacy Windows SMB services. In May 2017, WannaCry ransomware crippled 80 National Health Service (NHS) hospitals in Britain, forcing 19,000 appointments to be cancelled and costing the NHS a total of £92 million to remediate. One month later, NotPetya struck the servers of Nuance, a company that provides transcription services to hospitals. NotPetya caused Nuance's services to quietly fail, stopping tens of millions of medical transcriptions—including pre-surgery notes and changes to prescriptions—from being incorporated into the relevant patient files. Sutter Health, a healthcare system operating 24 hospitals and over 200 clinics, reported that within 24 hours the NotPetya attack on Nuance had created a backlog of 1.4 million changes to its patients' records. Nuance itself lost around $15 million as a result of NotPetya. In that respect, it got off easy; pharmaceutical company Merck, for example, experienced $870 million in losses, and the White House estimated that NotPetya damaged the global economy to the tune of $10 billion.

Yet another—and often-overlooked—risk to healthcare from legacy systems comes from legacy software embedded in medical equipment. In 2015, cybersecurity firm TrapX detected the MEDJACK attack vector, which targets embedded legacy systems in diagnostic equipment (e.g., CT scanners and MRIs), therapeutic equipment (e.g., an infusion pump), and even life support equipment (e.g., a dialysis machine). MEDJACK attacks take advantage of well-known exploits in older operating systems, such as vulnerabilities in Windows XP and Windows Server 2003 versions of the Service Host Process (svchost.exe) that were patched in subsequent releases of the operating system. These attacks often specifically ignore newer versions of Windows, which can block the attacks and are more likely to detect them. Although a MEDJACK attack can itself be used to edit or delete data from the compromised device, attackers usually use the device as a backdoor through which they can launch larger attacks, such as ransomware attacks. As of 2018, MEDJACK had undergone four evolutions, with MEDJACK.4 intrusions being especially hard to detect. It is difficult to ascertain how many hospital cybersecurity incidents can be attributed to MEDJACK specifically, but TrapX's report suggests that many common pieces of hospital equipment are vulnerable. To collect long-term data, TrapX installed software in more than 60 hospitals to trace medical device hacks. After six months, all 60 of the hospitals had compromised devices, many of which had been compromised by MEDJACK attacks.

Even when hospitals can afford new (or at least less-outdated) hardware, budget constraints often mean that hospital IT teams are either not sufficiently trained in proper cybersecurity procedures or are unable to effectively select security-conscious vendors. In October 2018, a hospital technology vendor, MedCall, misconfigured an Amazon S3 storage bucket containing around 10,000 files belonging to a client hospital. The misconfiguration left the files, which included the usual mix of PHI along with social security numbers and even recordings of patient evaluations, entirely open to and editable by the public. MedCall attributed the breach to the client hospital's poor security practices—an audacious claim given that not two weeks earlier, MedCall had similarly misconfigured another S3 storage bucket containing its own employees' PHI. While there is some encouraging evidence suggesting that hospitals have become apprised of the need to bolster their cybersecurity efforts, poor funding, legacy systems, and low expertise to continue to facilitate preventable cybersecurity breaches.

Supplementing the "Defend Forward" Strategy

In view of the relatively dismal state of hospital cybersecurity, what role might DOD's "defend forward" policy have to play in the healthcare sector? A capacious view of "defend forward" might encompass active target-hardening, in which the government would invest in improving hospital cybersecurity. Hardening hospitals against attack is not as contrary to the values of "defend forward" as it may initially seem. To "defend forward," DOD must be able to not only preemptively degrade an adversary's ability to attack, but also must be able to quickly detect intrusions and attacks and respond to them as swiftly as possible.

Accordingly, to harden hospitals against attack, DOD and HHS should cooperate to promulgate a rule establishing a standard, modern cybersecurity policy for hospitals. There is certainly a place for policymaking in "defend forward;" a well-crafted cybersecurity policy can effect substantial systemic improvements. For example, FireEye's 2020 report asserts that in the EU, there has been a marked reduction in dwell times, or the amount of time an intruder can spend in a secure system before being detected. FireEye suggests that this reduction is a result of the significant improvements and harmonization to data privacy and protection practices made by the GDPR. An analogous improvement to dwell times in the U.S. in conjunction with some capability for hospitals to report detected intrusions directly and promptly to the government could greatly enhance DOD's ability to determine which attackers it should attempt to degrade or counterattack, per the philosophy of "defending forward."

As a model for a new rule, DOD and HHS could use the report and set of technical volumes prepared by the Assistant Secretary for Preparedness and Response's Cybersecurity Act of 2015 Section 405(d) Task Group. The Task Group was a collaboration between public officials and private cybersecurity experts, and wrote its report with an eye for real-world application. The report was mostly released on December 28, 2018 and helps clarify what the healthcare industry standard for cybersecurity ought to be in view of many of the most cutting-edge developments. In particular, the technical volumes outline clear, actionable—and *adaptable*—standards for organizations to implement against a wide variety of cybersecurity threats. The report and manuals provide guidance for implementing MFA, email encryption, and end-to-end network encryption, all of which are standard for enterprises outside of the healthcare industry. Additionally, the report and volumes examine possible solutions to and protections from another major hospital cybersecurity threat: phishing. Perhaps most importantly, the report and technical volumes are based on NIST Cybersecurity Standards and thus supplement HIPAA with industry best practices—which continually evolve—rather than simply restating HIPAA or attempting to supplant it. DOD and HHS's new rule could simply require that hospitals comply with the standards articulated in the report and volumes, with some updates as innovations in cybersecurity take place.

The rule should also create a supplementary breach reporting requirement. Ideally, hospitals should be required to report major cybersecurity breaches to the Cybersecurity and Infrastructure Security Agency (CISA) within 12 to 24 hours of detection, to better allow the government to respond. Even at its best, the way in which OCR enforces the HIPAA Security Rule allows hospitals to decide with relative impunity exactly when they will report a cybersecurity breach, even as late as five months after discovering it. Given the speed with which cybersecurity incidents take place, the current requirement does not provide the government sufficient opportunity to take action against the attackers. A truncated requirement that hospitals report breaches to CISA would allow CISA to better fulfill its role as the national clearinghouse for cybersecurity infrastructure information. It would also enable CISA to better coordinate the activities of DOD and major hospitals in the case of cyberattacks against healthcare infrastructure. Finally, the increase in timely information collected by this reporting requirement could help DOD identify signs that a large-scale attack is underway, enabling it to "defend forward" against that attacker and potentially halt its activities.

To incentivize hospitals into quickly complying with the new DOD-HHS cybersecurity rule, DOD and HHS should request that Congress appropriate funds that can be used to upgrade legacy systems and hospital cybersecurity mechanisms. The funds would be directed at making sure every hospital meets the security "floor" designated by the rule. By helping to harmonize hospital cybersecurity, these appropriations would make the healthcare industry as a whole less attractive to attackers. There is much to be said for harmonizing hospital cybersecurity. For example, a 2018 academic publication in the Journal of Medical Internet Research authored by Mohammed Jalali and Jessica Kaiser of MIT Sloan School of Management concluded that "efforts to homogenize resource availability across hospitals reduce the likelihood of cybercriminal attacks." When DOD can rely on hospitals to resist and quickly report attacks to DOD, DOD becomes empowered to strike back and harass attackers per the strategy of "defend forward."

To round out this supplement to "defending forward," DOD and HHS should request that Congress establish a citizen cause of action against hospitals that fail to comply with the new rule. Currently, lawsuits against hospitals for cybersecurity breaches tend to fail for lack of standing. It is difficult for plaintiffs to demonstrate that they have been directly, specifically harmed by a hospital cybersecurity breach. Plaintiffs' PHI could be sold and affect them in a way that does not become clear until later. Because plaintiffs often cannot demonstrate standing, it is difficult for them to advance litigation to the point where courts can begin reviewing hospital cybersecurity practices. What this effectively means is that negligent hospitals can continue to put off upgrading their cybersecurity protocols, safe in the knowledge that no plaintiff will be able to demonstrate the hospital's negligence. To combat this, Congress could allow patients to sue hospitals when the hospitals fail to comply with the proposed new cybersecurity rule and that failure results in that patients' data being exposed in a breach.

To avoid retreading the past, this new cause of action would confer standing on any plaintiff whose PHI was affected by the breach, without the need for plaintiffs to show that they were materially harmed. Hospitals would then be unable to get litigation dismissed for lack of standing, and courts would be able to undertake an examination of hospital compliance with the standards in the proposed rule. Damages could be largely punitive in order to disincentivize noncompliance. Patients are the appropriate litigants for this particular task; it is, after all, their data at stake. Ideally, patient suits against a breached hospital would act as an acid test of that hospital's compliance efforts, conclusively demonstrating what kind of compliance is adequate and what kind is not. By exposing hospitals to potentially steep punitive damages for failing to be proactive insofar as cybersecurity is concerned, patients could force hospitals to cleave to the spirit of the rule rather than attempting to hide behind letter-of-the-law compliance.

* * *

The animating principle behind "defend forward" is that the best defense is a good offense. Yet rather unsurprisingly, especially in the hospital context, the best defense is actually a good defense. DOD and HHS can harden hospitals against attack by establishing through rulemaking a uniform national cybersecurity policy. Congress can ensure that DOD will fulfill its mission to "defend forward" in the hospital context by securing additional funding for hospital cybersecurity modernization and establishing citizen causes of action against hospitals that fail to comply with the new rule. Newly-hardened hospitals will be much more difficult for both nation-state adversaries and more mundane cybercriminals to attack, particularly without detection. This will enable DOD to more expeditiously and completely respond to attacks, which is the essence of "defending forward."

Background Readings

1. Defending Forward: The 2018 Cyber Strategy Is Here
Nina Kollars and Jacquelyn Schneider
https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/

2. *2019 HIMSS Cybersecurity Survey Final Report*
https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf

3. *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*
Yisroel Mirsky, Tom Mahler, Ilan Shelef, and Yuval Elovici
https://arxiv.org/abs/1901.03597

4. Cybersecurity in Hospitals: A Systematic, Organizational Perspective
Mohammad S Jalali, MSc, PhD and Jessica P Kaiser, MBA
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/

5. Hospital Hackers Seize Upon Coronavirus Pandemic – Pew Stateline
Jenni Bergal
https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/04/13/hospital-hackers-seize-upon-coronavirus-pandemic