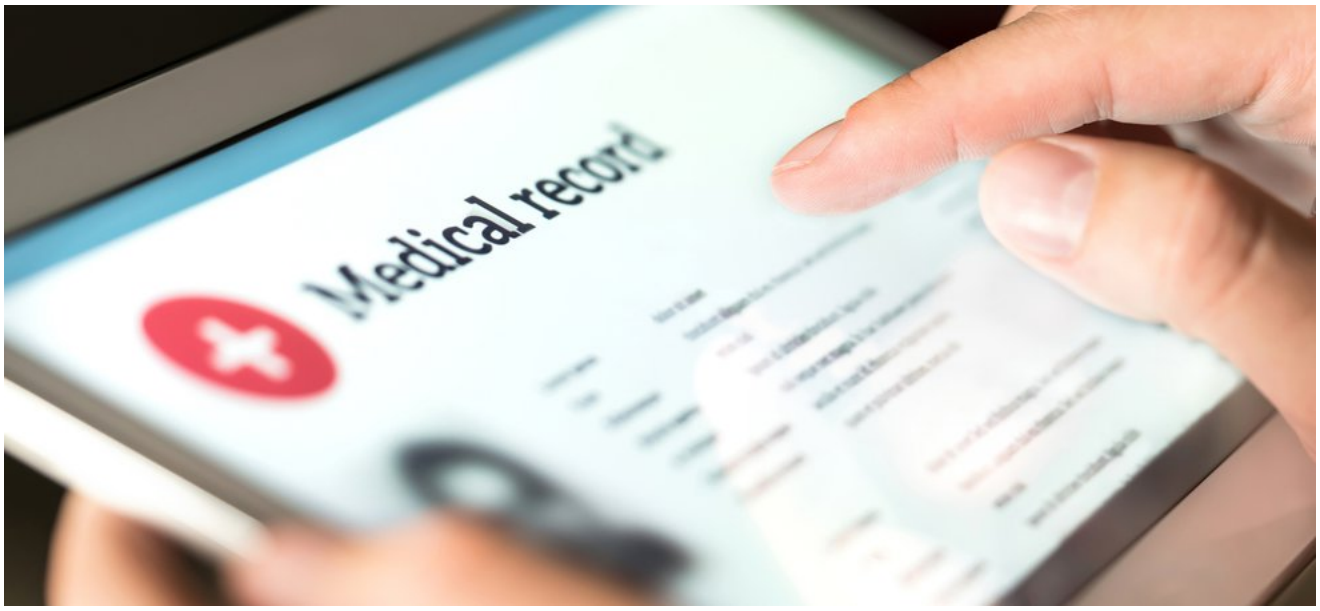
NEW AMERICA



October 2019

Do No Harm 2.0

Robert Lord & Dillon Roseen

Last edited on October 16, 2019 at 10:47 a.m. EDT

Acknowledgments

Special thanks also goes to Gabe Nicholas, whose extensive work in the final stages of this paper aided greatly in creating the finished product you hold today.

The authors would like to thank the countless independent privacy and security experts, healthcare practitioners, executive leaders in healthcare, and experts in artificial intelligence, information technology systems, and workforce development whose work made this report possible. Specific thanks go to those individuals who provided thoughtful commentary throughout the development of this project, including:

Laura Bate, Policy Analyst, New America

Rear Admiral Susan J. Blumenthal (Ret.), MD, MPA, Senior Fellow in Health Policy, New America

Daniel Bowden, VP and Chief Information Security Officer, Sentara Healthcare

Mark Combs, CIO, Steptoe and Johnson, PLLC

Carlos Cruz, SVP/Chief Compliance Officer, Tri-City Medical Center

J. Michael Daniel, President, Cyber Threat Alliance

Dante Disparte, Founder, Chairman and CEO, Risk Cooperative

Matt Doan, Cybersecurity Policy Fellow, New America

Matt Fisher, Partner, Mirick O'Connell

Michael Fried, CIO, Baltimore City Health Department

Chandresh Harjivan, Partner and Managing Director at the Boston Consulting Group (BCG)

David Holtzman, VP, Compliance Strategies, CynergisTek

Peter James, Founder, Amen Ra Security

Robert Morgus, Fellow, New America

Dr. David Mussington, Professor, UMD School of Public Policy and Board Director, (ISC)2

Mitchell Parker, Executive Director, Information Security and Compliance, IU Health

Michael Prebil, Program Associate, New America

Joy Pritts, Principal, Pritts Consulting

Lucia Savage, Chief Privacy Officer, Omada Health

John Schwartz, Chief Information Security Officer, Health Quest

Heidi Shey, Principal Analyst, Forrester

Dave Summitt, Chief Information Security Officer, Moffitt Cancer Center

Hussein Syed, Chief Information Security Officer, RWJBarnabas Health

Ian Wallace, Senior Fellow, New America

Beau Woods, Cyber Safety Advocate, I Am The Cavalry

Please Note: The affiliations of the noted individuals in no way indicate organizational endorsement of the recommendations in this report. Each of these individuals has merely provided commentary, insights and enhancements that we are very thankful for.

We also wish to acknowledge the supporters of the New America Cybersecurity Initiative whose support helped make this paper possible, notably the Citi Foundation (through their support to New America's Millennial Public Policy Fellows Program), Florida International University and the Hewlett Foundation.

About the Author(s)

Robert Lord is a fellow in New America's Cybersecurity Initiative and the lead adviser to the Healthcare Cybersecurity Project. Lord is the co-founder and president of Protenus, an analytics platform that leverages artificial intelligence to detect data breaches in healthcare. Before co-founding Protenus, Lord was an MD candidate at the Johns Hopkins University School of Medicine. Prior to medical school, Lord was an investment associate at Bridgewater Associates, the world's leading hedge fund. Robert received his A.B. in social studies, magna cum laude, from Harvard University.

Dillon Roseen is a law student at the University of Michigan School of Law. He was a Millennial Public Policy Fellow in New America's Cybersecurity Initiative and the staff lead for the Healthcare Cybersecurity Project. Roseen, from Peachtree City, Ga., was a Fulbright Scholar in Amsterdam where he conducted research on the intersection of law, politics, and international security and earned an LL.M. from Vrije Universiteit Amsterdam. Previously, he graduated with highest honors from the Georgia Institute of Technology.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

Contents

Contents Cont'd

Executive Summary

While this report is ostensibly about cybersecurity in healthcare, we hope it is remembered as yet another contribution to the broader body of patient safety literature in medicine, albeit an unorthodox one. Specifically, we aim to highlight the need to mitigate the risks to patient safety created by the growing integration of information technology and operational technology into healthcare, and to propose ways to mitigate that risk. The report takes as a core premise that there is great benefit to be had from technology adoption, but also that in order to achieve that benefit, action will be required to prevent those same systems—either maliciously or by accident—leading to patient harm. Recognizing that this is a complex systemic challenge, the report offers 17 actionable recommendations which we believe could make a real impact. These recommendations are organized across three pillars: culture, technology and workforce.

The report begins with a personal introduction by co-author Robert Lord which makes the case that information security should be at the heart of modern healthcare by pointing to Hippocratic Oath of "Do No Harm," which has long underpinned the work of healthcare professionals. Since the potential harms posed to patients today are not what they once were, he argues that "Do No Harm 2.0," requires significantly more attention and resources to be applied to cybersecurity by the healthcare sector.

Next, Chapter One—"Why Should We Care?"—gives a high-level overview describing the cybersecurity challenges and constraints facing the healthcare sector. Some of these challenges are unique to healthcare while others will be familiar to cybersecurity experts in other fields. The chapter will be most useful for those who want to better understand the cybersecurity threats the healthcare sector will face over the next five years. This chapter is designed to give action-oriented colleagues a set of arguments to support their efforts for change.

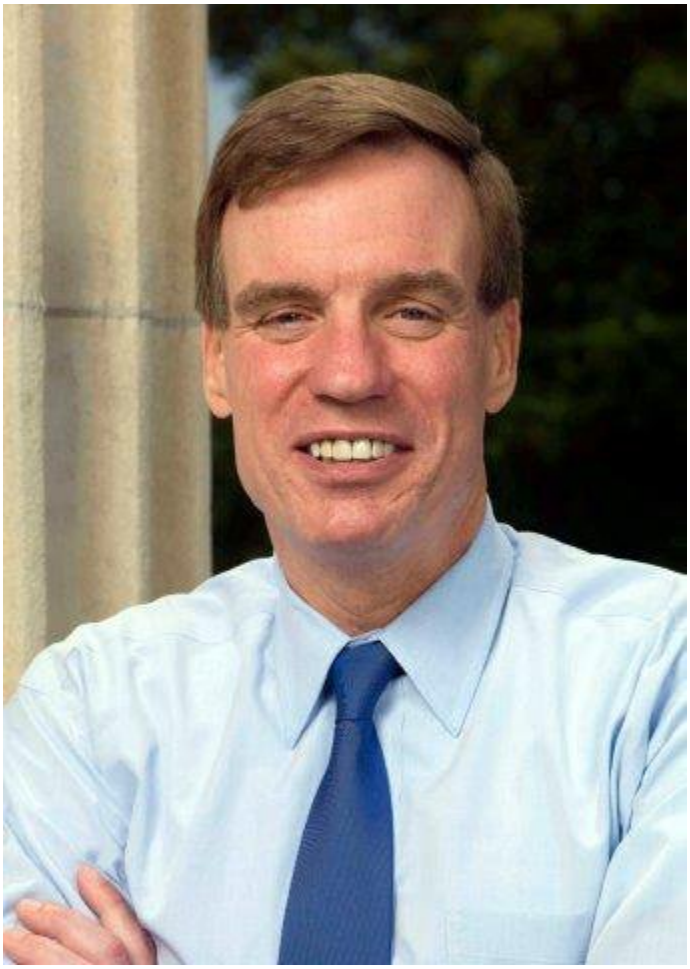
Chapter Two of this report—"How Did We Get Here?"—looks back at the major policies, technological innovations, and cybersecurity incidents that have shaped the current healthcare cybersecurity landscape. This chapter is for those who want to better understand the structural context underpinning technology and cybersecurity developments in the healthcare sector. By providing historical context, we hope to help ensure that future efforts will build on, rather than repeat, past attempts at improvement.

Chapters Three, Four, and Five constitute the major policy recommendations of this report. Each one tackles a set of recommendations centered on one of the three pillars mentioned above, culture, technology, and workforce. The policies in these chapters are relevant for policymakers in federal, state, and local

governments, as well as healthcare leaders who can shape the internal policies of their health systems and organizations.

The report concludes with a "call to arms" couched with optimism that this is a solvable problem if proper action is taken and appropriate resources are committed.

Foreword by Sen. Mark Warner



The WannaCry ransomware attacks in 2017 demonstrated that cyber-attack targets have moved from being concentrated on finance and government entities, to other industries like health care, telecommunications, and logistics, with the attack surface growing to include vulnerabilities in hardware as well as software. The rapid adoption of technology in health care has the potential to improve the quality of patient care, expand access to care, and reduce wasteful spending. However, such technology also has the power to put patients at risk as it facilitates the proliferation of valuable personal health care data. To support the benefits of health care technology, we must also effectively protect patient information and the essential operations of our health care entities. Furthermore, escalating cyber-attacks against health care entities are not just data or device security issues— they are a patient safety concern.

Recognizing that cybersecurity is an increasingly complex issue that impacts the health, economic prosperity, national security, and democratic institutions of the

country, I helped establish the Senate Cybersecurity Caucus in June of 2016. The bipartisan Caucus serves an educational resource to help the Senate more effectively engage on cybersecurity policy issues, and to highlight the most pressing information security challenges facing the United States. With the ongoing rise in ransomware and other cyber-attacks, my colleagues and I have noticed that the health care industry is increasingly targeted. It is more important than ever to better understand how cybersecurity and health care interact.

Robert Lord and Dillon Roseen's report, "Do No Harm 2.0," is a valuable effort to bring awareness to the issue of cybersecurity and health care. It underscores the fact that information security is not just an IT issue, but also a patient safety issue. It describes the state of the threat, the importance of the problem, and provides a number of potential policy remedies for Congress to consider. As a longtime advocate for the importance of addressing cybersecurity vulnerabilities in health care systems and organizations, I thank the authors for bringing much-needed attention and thoughtfulness to the issue, and hope that it will receive the consideration it deserves.

U.S. Senator Mark R. Warner (VA)
Co-Chair Senate Cybersecurity Caucus

Personal Introduction by Robert Lord

The Big Idea

Earlier in my career, I attended medical school (though I never graduated, much to my parents' chagrin), and while doing so was privileged to work at a clinic in Baltimore that served primarily HIV-positive patients. It was a formative experience for me. I found that patients would often risk their own health outcomes to avoid having their information shared and their diagnosis exposed to the community.[1] Some would miss appointments or skip doses of life-saving medication to avoid colleagues learning of their illness. A few patients were so concerned about the privacy of their diagnosis that they entirely ceased care, potentially costing them their lives. HIV-positive patients are far from the only individuals with sensitive diagnoses. Most people, over the course of their lives, will accumulate information in their electronic medical records (EMRs)[2] that they would rather not share with the world.

The core premise of this paper is that poor cybersecurity and privacy practices now represent a major threat to patient safety, and as such, deserve much greater attention from physicians, senior leaders in the healthcare sector, and policymakers. This is not a new insight in the field of healthcare cybersecurity, having been put forward by many leaders in the field, but it has a special resonance for me.[3]

During medical school, I spent a significant amount of my time working in the field of patient safety research, particularly in Intensive Care Units. The work we did there has remarkable parallels to the work my colleagues and I now do in cybersecurity and privacy. Through my work at Johns Hopkins,[4] in one of the finest patient safety research groups in the country, I learned that three key factors define the success of a patient safety intervention: technology, workforce, and culture. Those are exactly the components of a successful cybersecurity strategy.

Technology, broadly speaking, has been a powerful force in patient safety, but it's not always the most advanced new artificial intelligence system that wins the day. Indeed, the work of checklists with the Stop BSI campaign, designed to combat bloodstream infections, was the technology we needed back in the early 2000s.[5] However, as this work has continued to advance, so has the work of AI and machine learning in predicting and preventing patient safety events, such as preventable septic shock or errors in emergency patient triage.[6] The need for appropriate technological innovation is no different in healthcare cybersecurity, where we need both the basics of good frameworks, as well as the augmentation and assistance that comes with transformative technology.

Culture change is also a powerful transformational tool, and perhaps the most critical of all interventions in patient safety. Whether creating safe harbors for reporting medical errors so clinicians can learn from their mistakes and others', or developing more robust accountability for handwashing, it is the challenge of culture change that defines both the greatest opportunities and challenges in healthcare. Similarly in cybersecurity, we have a great need to change viewpoints, accountability, and entrenched practices, and we propose in this paper some pathways to get there.

Changes in our workforce are also a powerful driver for a sustainable future of improved patient safety. An awareness of patient safety is now embedded in medical curricula across the country, including the one that I was privileged to attend years ago. Students have opportunities to engage early, and training in best practices is both freely available and valued by academia. With each new generation of clinicians, more and more awareness builds of the importance of mitigating preventable errors, and our role in tackling these errors. So we must work to build both awareness in our workforce, as well as create the pipeline and training that keeps our healthcare cybersecurity workforce strong and at the cutting-edge of the challenges it will face.

Thus, to me, there is no stretch of the imagination or clever rhetorical flourish necessary to think of good cybersecurity and privacy as a matter of patient safety —it is, in every way, an essential component of reducing the preventable harms that can be predicted and prevented, if we have the will to do so.

Despite a near-consensus among cybersecurity professionals that the healthcare sector faces a cybersecurity crisis, too often we assume that innovations in patient care will be unambiguously beneficial for a patient. There is increasing evidence[7] that these advances often come with cybersecurity risks that potentially expose patients to significant harm. Failing to mitigate medical cybersecurity vulnerabilities places patients and hospitals at risk of incurring real financial, reputational, and physical harm.

A core principle of medical ethics spanning as far back as the ancient Greek physician Hippocrates states *primum non nocere*, "first, do no harm."[8] This principle centers on a doctor's obligation to prevent harm from befalling a patient. It requires a careful balance between the potential benefits and risks of a treatment. The benefits of these emerging healthcare technologies must be balanced with the attendant cybersecurity risks to ensure that a new, dynamic version of the "Do No Harm" principle can be upheld. In my experience, many parts of the United States healthcare system are at serious risk of failing to adhere to that principle. Hence the "Do No Harm 2.0" title of our project.

Healthcare cybersecurity has been a passion of mine for many years, first as a medical student and then as an entrepreneur. But I also realized some time ago that change at scale would require policy change. This report is an attempt to

affect that, and I am grateful to have the opportunity to do that with my colleagues at New America, and particularly my fantastic coauthor Dillon Roseen. Neither of us believe that the ideas in the paper are revolutionary, but we do think that together they represent a practical and much needed path to a better future.

A Note on our Approach

Our goal is to set out a pathway to action, not to cut across good work that is already being done in this space. As such, we stand on the shoulders of many groups and individuals who have been thinking about these challenges for years —we hope to consolidate many great ideas in healthcare security and privacy in order to operationalize them.

In pursuit of that goal we decided to pursue a twin track approach—both to emphasise the big, bold idea that it is high time that cybersecurity in healthcare should be more widely treated as a patient safety issues. But we are also mindful of the fact that visionary aspirations alone will not get us where we need to go. And so through many interviews and much research identified and refined a set of 17 practical recommendations that, if implemented, would go a long way to realising that vision.

Indeed, the goal of this project is to set out a series of specific policy measures that bring cybersecurity and privacy in the healthcare sector to where they need to be five years from now. While some of these ideas are new, many of them build upon the hard work of experts and organizations who have been tackling these problems for decades. This project will ultimately challenge the field to think critically about where healthcare is headed over the next five years and how today's policy solutions can mitigate future challenges. Do No Harm 2.0 offers a number of detailed policy recommendations that together will serve to secure the health systems of tomorrow.

Our recommendations are based on a review of existing policy guidance, including from the June 2017 Health Care Industry Cybersecurity Task Force Report; governmental and industry organizations like the National Institute of Standards & Technology (NIST), the United States Department of Health and Human Services (HHS) (including the Office for Civil Rights (OCR), the Healthcare Industry Cybersecurity (HCIC) Task Force and more), the Healthcare Information Sharing and Analysis Center (H-ISAC), Healthcare Information Trust Alliance (HITRUST), the College of Healthcare Information Management Executives (CHIME), the American Hospital Association (AHA), the American Medical Association (AMA), the Healthcare Information and Management Systems Society (HIMSS), the United State Food & Drug Administration (FDA), and many others; background research, including desk research, input from frontline practitioners, independent privacy and security experts, and executive leaders in healthcare; and consulting New America's network of experts in

healthcare, cybersecurity, artificial intelligence, and information technology systems. Many past reports have taken a broad look at the complex, interconnected issues faced by the healthcare sector, so in the spirit of "Do No Harm," this paper will focus specifically on the risks faced by providers and health systems.

This work comes on the heels of both the FDA's guidance on medical device cybersecurity,[9] the Cybersecurity Task Force's Health Industry Cybersecurity Practices,[10] and the Healthcare Sector Coordinating Council's Joint Security Plan,[11] three powerful and practical documents that provide helpful insight into hospitals' on-the-ground challenges and how to tackle them. We do not seek to replicate or replace any of this work—rather, we focus on 1) specific policy change recommendations and 2) the next five year time horizon for evolving our field.

Naturally, this approach has affected the way we have written the report. First, we have consciously targeted our recommendations at the healthcare community, and healthcare policymaking experts. So, while we very much believe that it can and should serve as a guide for newcomers to the area, we make no apologies for the fact that the analysis and argumentation assume at least a degree of understanding of the healthcare industry.

Second, this approach also means that we have deliberately made our recommendations specific to the sector. That is not intended to suggest that all of the challenges facing the sector are unique to healthcare. In fact, use of generally accepted cybersecurity best practices, such as adoption of the National Institute of Standards and Technology Cybersecurity Framework[12] (designed for use across critical industry sectors) should be a given for all organizations in the sector. However, we have consciously focused on healthcare specific recommendations, because that is what we believe is currently missing from the conversation.

Structure

This project uses a three pillar framework to address the privacy and security needs of the healthcare sector. The three pillars, which respectively correspond to Chapters Three, Four, and Five of this report, are:

- *Culture.* Crystallizing cultural norms in healthcare to ensure trust between patient and provider
- *Technology.* Identifying technological opportunities and challenges related to cybersecurity and privacy facing the healthcare sector
- *Workforce.* Building a skilled healthcare cybersecurity labor pool for the future

A Note on Conflict of Interest

Finally, I must acknowledge that as a cofounder of a healthcare compliance analytics company I have a vested interest in promoting better healthcare in cybersecurity, as some of our products solve problems in this realm. I do not believe that that undermines my ability to argue for the importance of better cybersecurity, or that it should be treated as a patient safety issue. Indeed, that was part of my motivation is leaving medical school to establish my company. However, I am very conscious of the need to avoid any conflict of interest, and my co-author Dillon Roseen and other colleagues at New America have been scrupulous in ensuring that none exists.

Chapter 1: Why Should We Care?

I. Cybersecurity Is A Patient Safety Imperative

For healthcare professionals, patient safety is paramount, but even simple treatments can be far from risk-free. For example, in the interest of seeking a diagnosis, a doctor may have to order an imaging study or test that carries its own risks (e.g., a CT with contrast might cause an allergic reaction). Over the years, however, as the medical profession has developed a better understanding of how these tests are used, we can weigh the benefits and risks, and also develop methods to reduce the risk of an adverse outcome (e.g., doing a thorough patient history to assess the risk of the aforementioned allergy).

So it is with healthcare information. To do their jobs, healthcare professionals need to collect and analyze the most intimate details of our personal lives. Managed correctly, especially given the new technology now available, collection of that information can contribute greatly to the recovery of a patient. But without the correct protocols in place, that very same information can lead to inadvertent harm, possibly in excess of the original reason for seeking medical attention.

This is what we mean by saying that cybersecurity is a patient safety issue, and this report is intended to suggest ways in which the healthcare industry can help patients benefit from the extraordinary potential of informational system to enhance their well-being, while simultaneously mitigating potential risks. To do that we first need to understand those risks.

Information security professionals often say that the goal of cybersecurity is to maintain three qualities of a system: 1) confidentiality, meaning that access to information is restricted only to authorized users; 2) integrity, meaning the information is trustworthy and accurate; and 3) availability, meaning authorized users can quickly and reliably access information.[13] These three qualities may seem abstract from patient well-being, but in reality, they are crucial to ensuring quality care.

Healthcare providers need to maintain the confidentiality of their patients' data not only to prevent medical identity theft, but also to assure patients that they can safely share sensitive health information. A study by the Office of the National Coordinator (ONC) found that of patients who did not believe providers reasonably protected their electronic health records, 33 percent had at some point withheld information from a provider due to privacy or security concerns (as opposed to 7 percent of the overall population.)[14] As knowledge of cyber risks percolate through popular culture over the next five years, the number of patients who withhold potentially important information from providers could increase if

the perceived security does not improve. (Addressing only the perception part of this by underreporting breaches could dramatically backfire.)

Attackers who gain access to a piece of health technology may be able to compromise its integrity by manipulating the data it collects or transmits. Providers with invalid information may misdiagnose and mistreat patients, with potentially grave consequences. Wildly inaccurate data or altered biomarkers that ought to be immutable may cause other medical equipment to malfunction. After providers learn that some data is compromised, it still may take countless man-hours from IT staff and caregivers to restore accurate information, and only then the information that has not been irrevocably lost.

Even a short disruption or slight slowdown in the availability of health data can be the difference between life and death. Healthcare providers may need to access an electronic health record (EHR) or communication tools to get information on a patient in a time sensitive condition. Attackers are increasingly taking advantage of this necessity with ransomware attacks, remotely locking hospital computers until a ransom is paid. According to McAfee, ransomware attacks in the healthcare sector increased by 210 percent between 2016 and 2017, [15] and as of Q2 2018, healthcare is the most targeted of any sector for cybersecurity attacks.[16]

Before introducing the policy solutions that can help steer healthcare towards a more cyber-secure future, it is useful to understand the historical context that shaped the current healthcare cybersecurity landscape. The following chapter provides a historical overview of the events and policies that underpin the current state of cyber insecurity in the healthcare sector.

II. The Case for Urgent Action

What adds urgency to this issue is that the use of information systems in healthcare has increased markedly in recent years, and often the pace of that change has run ahead of ways to mitigate the risks that these developments create. Alongside the increased adoption of networked medical devices, EHRs, and wirelessly-augmented health infrastructures, there has also come an increase in cybersecurity vulnerabilities. These vulnerabilities, whether exploited or not, disturb the delivery of healthcare by weakening this aforementioned, essential foundation of trust. Medical technophobia is not the solution. New medical technologies have improved patient outcomes and helped health systems meet the 21st century demands placed on them. As such, the healthcare sector needs to think systematically about cybersecurity as a necessary trust-building measure with profound implications for patient privacy and safety.

The dangers to the healthcare sector of exploitable cybersecurity vulnerabilities are not imagined. Already, security researchers have demonstrated that

malicious actors can exploit vulnerabilities in implanted and networked medical devices that deliver life-supporting functions, like ventilators, infusion pumps, pacemakers, and monitors.[17] An often underappreciated threat is the loss of a patient's protected health information (PHI) as the result of a data breach. In many cases, stolen or inappropriately viewed records reveal patient names, addresses, social security numbers, health insurance information, diagnoses, procedure codes, intimate medical images, and financial data.[18] Beyond flagrantly violating patient privacy, the information contained in stolen records can be used to threaten patients' safety, compromise identities, and fuel fraudulent business or pharmaceutical practices.[19] This is unacceptable.

III. The Cybersecurity Risk Landscape Facing the Healthcare Sector

Healthcare Cybersecurity in Context

Healthcare is far from the only critical infrastructure[20] sector that is vulnerable as a result of its dependence on information systems. Indeed, as a starting point, healthcare organizations would do well to begin any systematic analysis of their security by adopting the NIST Cybersecurity Framework—designed for use across sectors. However, like any other sector, healthcare has its own peculiarities, not the least of which is that rapid access to a patient's information can often be what makes the difference between life and death. Given the complexity of patient care, the sort of access controls that might work in other industries are often not appropriate.

In other words, the primary mission of the healthcare sector is to provide timely, longitudinal, and personalized care to patients, on the basis that all lives are of equal value.[21] To fulfill this mission, healthcare professionals must be able to quickly and easily share and collaborate using patient information. In the operating room, the emergency department, and across healthcare environments, medical professionals need accurate and readily available patient data to make split second, life and death decisions.

These are complex problems, often requiring the balancing of different risks. For example, in some cases it is the lack of easy access to information for the right people that causes the most problems. OCR has begun to respond to these challenges in care coordination, as a part of its responsibilities to enforce and interpret HIPAA (the Health Insurance Portability and Accountability Act, which defines the privacy and information access rights of patients, among many other areas). On top of the ordinary waiving of HIPAA sanctions to help hospitals respond to natural disasters, OCR is considering rules (most recently through a December 2018 Request for Information[22]) to allow for "good faith" disclosures of patient data without their consent in emergencies like drug overdoses.[23] But in solving one problem, we risk creating others. Though this rule could improve health outcomes, it could also risk the privacy of economically vulnerable

patients, particularly if the healthcare provider uses poor cybersecurity practices. As we move more towards value-based care and expand care coordination, we must be thoughtful about the new vulnerabilities these practices can incur. Nevertheless, it is our contention that too often the cybersecurity risk is not properly or fully addressed.

Vulnerabilities and Consequences

No matter the type of care, healthcare providers require full and immediate access to patients' health records in order to properly tailor their treatments. Otherwise, providers risk exacerbating previous injuries, provoking allergic reactions, or otherwise harming a patient. Recent efforts have sought to improve patient health outcomes by facilitating the sharing of healthcare information. Technological advancements to this end include the shift to EHRs, the adoption of wirelessly connected medical devices, and the use of big data analytics to identify public health patterns. More providers, staff, and affiliates now have easier access to a greater volume of patient data than ever before, and this trend is accelerating (see Chapter Two).

But the more access points a health technology system has, the more difficult it is to ensure the cybersecurity of the whole system. One unpatched vulnerability on one device may allow an attacker to leapfrog through a health system's entire technological infrastructure, potentially crippling an entire hospital network.[24] Allowing more professionals or other individuals to access these systems makes it more difficult to track user activity, and a single unmonitored insider can lead to the theft or exposure of millions of intimate patient health records.[25] Ever-increasing amounts of data that health technologies collect may make health systems more appealing targets to threat actors.

Technological advancements are ushering in an exciting new age of medicine, and promising innovations should continue to be developed. However, healthcare leaders must balance the attendant cybersecurity risks that arise in the wake of such rapid technological change, or else patients will be harmed and their trust in the healthcare sector will deteriorate. Some of the costs that arise from these risks are described below:

Medical Costs

- Direct patient harm (e.g., a wirelessly exploited insulin pump delivering a fatal dose of insulin or prescribing a patient the incorrect medication as the result of a manipulated electronic patient record)

- Indirect patient harm (e.g., delayed or cancelled medical appointments, closure of hospitals, diversion of ambulances following IT systems failure)

- Medical identity theft, which is especially costly given the permanence, sensitivity, and value of health data and potential delay in discovery. Identity theft can also lead to direct patient harm as a result of duplicate records resulting in misdiagnosis or poor treatment.[26]

- System-wide operational disruption

Financial Costs

- Legal fees and penalties imposed as the result of a cybersecurity incident or data breach

- Credit-based identity theft resulting from EHR compromise, and costs for providing continuing identity theft protection

- Restoration or purchase of new information technology systems as the result of a system failure

- Fraudulent medical claims, including of prescription drugs, insurance, and Medicare and Medicaid

- Stock manipulation based on undisclosed vulnerabilities, incidents, and PHI

Reputational Costs

- Loss of public trust in the healthcare system

- Public HHS investigations, corrective action plans, and national exposure of potentially embarrassing and preventable information system failures

Moral or Ethical Costs

- Violating patient privacy and dignity

- Failing to provide immediate and personalized care, exposing patients to preventable harms

- Breaking the law under HIPAA

So what behaviors incur these cyber risks? Examples from a report by the Health Care Industry Cybersecurity Task Force show that they range from the technological to the human.[27] Poor network security, off-the-shelf software with

insecure default settings, and failing to install security patches on older, vulnerable devices can all allow attackers to exfiltrate patient data (more about technological vulnerabilities will be covered in Chapter Four). Meanwhile, uncontrolled distribution of passwords and improper disposal of patient data can allow employees unauthorized access. To fully understand these cyber risks though, it is important to know who the humans are behind the threats to the healthcare sector.

Threats: External and Internal

External cybersecurity threats are often the first that come to mind when thinking of risks facing healthcare. However, as the 2018 Verizon Data Breach Investigations Report (DBIR) notes, healthcare is the only industry where cybersecurity incidents are caused more often by insiders (56 percent) than outsiders (43 percent).[28] Insiders can take the form of employees, vendors, affiliates, or individuals who have somehow accessed legitimate credentials in order to compromise hospital systems. The actions they take can range from naively dangerous to existentially catastrophic. Cybersecurity experts observe that many attacks combine external vectors with internal actors, such as phishing or social engineering attacks.[29] Here, we examine the threats to healthcare cybersecurity in these two broad categories: external and internal threats.

External Cybersecurity Threats Facing the Healthcare System

As the name suggests, external threats originate from outside of a healthcare organization. Cyberattacks perpetrated by external actors involve infiltration of a healthcare organization by exploiting vulnerabilities in the software or hardware of connected medical devices, EHRs, and supporting systems. Attackers can deploy malicious code to gain entry to healthcare databases,[30] steal millions of protected health records,[31] demand money in exchange for health data and medical devices being held hostage,[32] and even prompt widespread disruption or chaos by crippling entire health systems.[33]

Healthcare providers—from stand-alone practices in Manhattan to enormous Integrated Delivery Networks (IDNs) in St. Louis—are regularly targeted by organized hacking groups. HHS maintains a database of breaches[34] that have been reported by health organizations (as they are legally required to do)[35] and the picture is bleak, especially when one includes industry analyses that incorporate many cybersecurity events that HHS misses. According to one such analysis of incidents from 2017, nearly 3.5 million patient records were stolen in the 144 cyber incidents for which data is publicly available.[36] While the total number of stolen records decreased from 2016 to 2017, the number of ransomware and malware attacks more than doubled.[37] Ransomware[38] and other malware attacks are some of the tactics most commonly used to target healthcare

organizations, but ransomware is by far the most common form of malware attack at 85 percent.[39]

A common vector for attacks like ransomware is phishing, or the use of infected emails and texts to gain access to a system. The Health Information Sharing and Analysis Center (H-ISAC) and security firm Agari recently found that more than half of the emails purportedly sent from healthcare organizations are fake, making healthcare the sector most targeted by fake emails.[40]

What does all of this tell us? The connectedness of the healthcare ecosystem leaves it vulnerable to massive, scaleable attacks capable of compromising protected health information and disrupting patient care and groups or individuals willing to exploit that vulnerability exist. Healthcare executives agree. In the recent 2018 HIMSS Cybersecurity Survey of healthcare executives, data breaches and hacking, which includes malware, ransomware, and phishing attacks, were named as the top cybersecurity threats facing healthcare organizations.[41]

Internal Cybersecurity Threats Facing the Healthcare System

According to the 2018 Verizon DBIR, healthcare is the only industry vertical where there are more insiders that cause a data breach than external actors.[42] Insiders, employees, and other intended users of an electronic health system, pose a unique risk to healthcare because they have legitimate access to healthcare information and thus are not subject to traditional, externally-facing cybersecurity defenses. There is also a significant fear that restricting access to data may hinder care, impeding such controls as role-based access control. Moreover, insiders have a thorough understanding of where vulnerable data may reside and possible vulnerabilities that exist within a wide array of systems that they use every day.

An insider incident or insider attack occurs when an individual or group within a healthcare system violates the law by improperly accessing protected health information or taking advantage of a medical cyber-physical system, such as a smart operating room or an implantable cardioverter defibrillator. Given the level of legitimate access insiders have to protected health information, it can be difficult to identify when an insider is abusing their access privileges. In some cases, insider threats can go undetected for astonishingly long periods of time—in one example, an undiscovered vulnerability allowed employees at an Indianapolis hospital to inappropriately access "current and former patients' social security numbers, contact information, diagnosis, treatment and health insurance" information for over three years.[43]

Insider incidents can be intentional, negligent, or malicious, but all three can be equally detrimental. It can be as simple as an employee checking on a relative's

record or as complicated as stealing thousands of tax returns. It can happen from a health professional not following protocol, by accidentally misplacing a patient's file or discarding a computer system without properly removing patient information. In 2017, nearly 800,000 patient records were compromised as the result of accidental insider errors.[44] Not all insider incidents are so innocent—potential reasons why an insider might intentionally and unwarrantedly access patient data vary as widely as the incidents themselves.

One reason could be to sell personal medical data on the darkweb,[45] as medical data is a "gold mine for vendors of stolen data" that operate on the darkweb.[46] Despite the influx of stolen health data flooding dark web markets in recent years, demand is still high. In 2017, records sold for anywhere from $20 to $50 or more per record depending on the value of the record to a buyer.[47] For comparison, "basic stolen identity information on a US citizen, which only includes the Social Security number, full name, and birth date, can range from $1 to $8 per person."[48]

Selling medical data is particularly harmful for patients because much of the information contained in a medical record is immutable, such as biometric data. The immutability of biometric data, like blood type, psychiatric history, and specific drug allergies, distinguishes it from other updatable information, like a password or credit card number. This means that a single compromised record can negatively affect an individual for the rest of his or her life. Moreover, stolen medical records contain a wealth of information, some of which is not even related to an individual's health. Emergency contact information can be used to guess the answer to security questions, billing and insurance information can be compromised leading to fraud, and embarrassing diagnoses can be used to extort or blackmail individuals.

Some insiders might unlawfully access patient information simply out of curiosity. The moment a new employee starts at a health system, they likely gain near-ubiquitous access to the health records of millions of patients. While the vast majority of health workers treat this responsibility with respect, some yield to the temptation. A physician may snoop into her ex-husband's psychiatric reports or a nurse may peer into his girlfriend's sexual and reproductive health history.[49] Employees may look up the medical history of celebrities that have come through their doors,[50] as happened to Kim Kardashian and former Rep. Gabrielle Giffords.[51] Insiders might even systematically steal medical records for use in filing false tax claims.[52] One author recalls the fear he and his colleagues had at entering in sensitive patient information, knowing that despite the hard work of the HIPAA privacy office, anyone of his co-workers could view the information with relative impunity.

What does all this tell us about insider threats? Namely, that insider threats pose a unique risk to the healthcare sector simply because employees are granted legitimate access to so much patient information. As such, identifying an insider

breach is more difficult and often takes longer. The scale of an insider breach can be just as harmful as one caused by an external hacker, particularly because insider breaches are so hard to spot. The costs associated with internal and external cyber attacks are high, affecting patients and healthcare providers to varying degrees depending on the scale and success of each attack.[53]

Chapter 2: How Did We Get Here?

Before introducing the policy solutions that can help steer healthcare towards a more cyber-secure future, it is useful to understand the historical context that shaped the current healthcare cybersecurity landscape. The following section provides a brief historical overview and timeline of the events and policies that underpin the current state of cyber insecurity in the healthcare sector.

The story of the last decade of healthcare privacy and security is one that is defined by both progress and tragedy, often in parallel. With the broad rollout of EHR technology, driven by meaningful use incentives contained in the HITECH Act of 2009, the capacity of healthcare infrastructure transformed to capture and access patient health data electronically.[54] However, this transformation came at a great cost—the creation of a slate of privacy and security vulnerabilities that are only beginning to be addressed. Likewise, the burgeoning of new wirelessly connected medical devices,[55] sometimes referred to as the medical Internet of Things (mIoT), increased healthcare's reliance on medical data to improve chronic and diet-related illnesses,[56] predict disease outbreaks,[57] and create strategic benefits driven by big data analytics.[58] The use of algorithms and big data has also enabled clinicians to, with extraordinary accuracy and efficiency, diagnose, and treat diseases including skin cancer, cardiovascular disease, and retinopathy (which causes blindness), and predict a patient's likelihood of deteriorating or dying.[59]

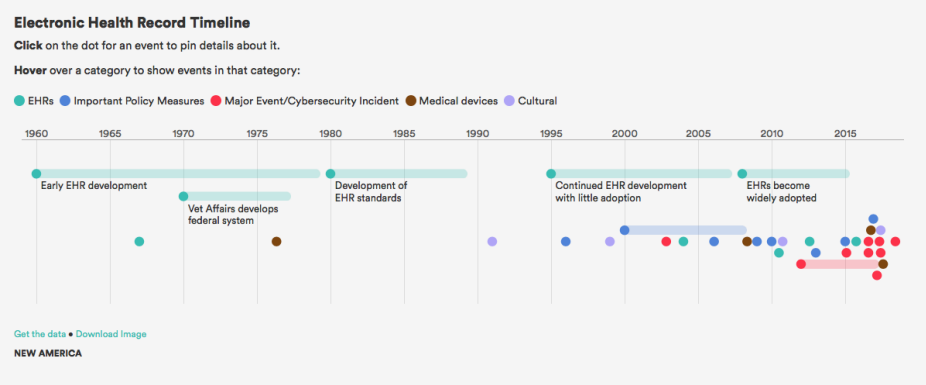
While many efforts were focused on improving patient care and interoperability —and appropriately so—this forward sprint neglected the concomitant deployment of technologies that would ensure these systems were secure, and that the data held within them was not accessible to individuals who had no use for it. As a result, the system created hundreds of millions of vulnerable digital medical records, and innumerable vulnerable devices and other entities, all of which led to a vast number of attacks over the past decade.

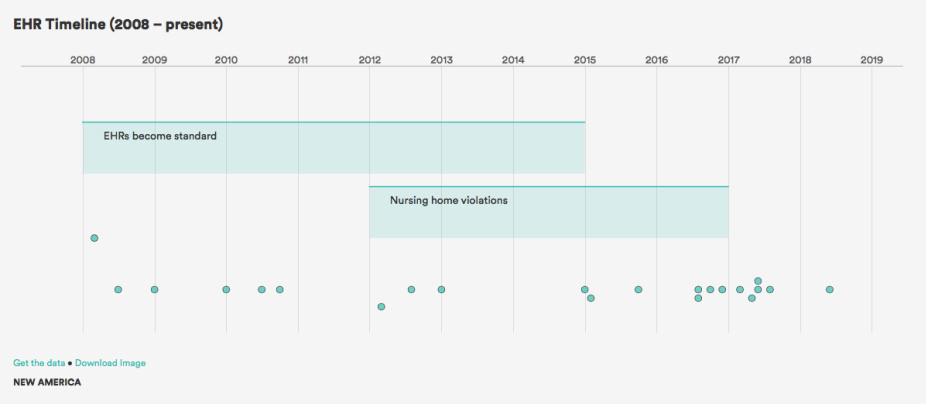
As Figure 1 demonstrates, the transition to EHR started slowly, but an explosion occurred in 2009, and with it, an attendant explosion of both large and small cybersecurity events, all of which had the potential for devastating impact.[60] Since *To Err is Human*, the seminal report on patient safety and medical errors that defined a generation of clinical research, the industry has experienced tremendous improvement in attentiveness to patient safety and medical errors.[61] However, only in the last few years, has some of this research related to the safety and dignity of patients and how this is impacted by cybersecurity and privacy vulnerabilities.

We separate out the pre-2008 and post-2008 era largely because of the significant transformation in healthcare technology that occurred in 2009 with

the HITECH act. This massive incentive program (in combination with other secular trends in the space) fundamentally changed the digital landscape, creating new opportunities and new vulnerabilities.

Figure 1: The Events, Policies, and Technologies That Have Affected Healthcare Cybersecurity





Chapter 3: Culture

I. Summary

Any attempt to positively transform cybersecurity within healthcare must be informed by an understanding of the cultural idiosyncrasies of the healthcare sector. By understanding the culture of healthcare from the start and identifying instances where the prevailing culture may directly conflict with beneficial cybersecurity measures, policy recommendations may be offered that both align with and shift cultural norms to ultimately support a healthy cybersecurity posture.

Atul Gawande's book *The Checklist Manifesto* speaks eloquently of the importance and challenges of even simple culture change, through the mechanism of preoperative surgical checklists.[62] While there are many important points made in the book, fundamentally the work of patient safety is around culture change. For instance, much of the process and procedure added by presurgery checklists was focused on getting nurses, doctors, and anesthesiologists to communicate and share goals more clearly. This simple act of going through a checklist together aligned them and improved their dialogue, a major contributor to the lives saved from these interventions.

This chapter begins with an overview of the aspects of healthcare's culture that affect the sector's overarching approach to cybersecurity. Some of the specific cultural challenges in healthcare are summarized in the table below:

Table 1: Summary of Healthcare Culture Challenges

Area	Unique Characteristic or Challenge
Diversity of healthcare stakeholders	Huge range of healthcare organizations, from single physician practices in rural localities to large IDNs with 100+ hospitals
Internal information sharing	Extremely open, academic culture of collaboration. Sharing of patient case details amongst healthcare employees is necessary to support mission. Few traditional role-based access controls.
External information sharing	Many stakeholders in healthcare who may need access to near- complete records (clinical partners, payers, government agencies, etc.)

Area	Unique Characteristic or Challenge
Internet of Things	Life-supporting medical devices that can be lethal if misused. Legacy devices introduce new security risks and privacy implications under HIPAA due to the collection and storage of sensitive data.
Lopsided digitization between clinical and infrastructural technology	Slow adoption of improvements to technologies that are not clinical devices and provider-driven purchases (i.e., the "shiny new thing"), but rapid and untested adoption of some patient-centered items.
Personnel	Professionals are generally non-technical but continuously interacting with sensitive technology. Reporting structures differ across healthcare organizations, often leading to poor responsibility and accountability over cybersecurity. Sometimes arbitrary cleavages between siloed privacy and security teams.
Budget	Highly-constrained and low-margin (mostly nonprofit) providers. No standard benchmark on the appropriate allocation of resources for cybersecurity per unit of scale in a health system. However, it is worth noting that insufficient cybersecurity budgets also exist at high-margin health systems.
Threat landscape	Insiders pose the greatest threat to healthcare organization in terms of data breaches; external threats pose the greatest risk with regards to ransomware/malware attacks against medical devices.[63]

To address these challenges, the chapter offers policy recommendations for policymakers in federal and state government, as well as healthcare industry leaders. Our cultural policy recommendations are:

1. The Department of Health and Human Services Office for Civil Rights should showcase health systems with innovative privacy and security programs (3.1)

2. Provide multi-tiered information sharing for healthcare's diverse practice environments (3.2)

3. Develop the cybersecurity equivalent of the nurse-to-patient ratio (3.3)

4. Hold boards of directors responsible for healthcare privacy and security (3.4)

5. Ease regulations to enhance the sector's resource sharing capabilities (3.5)

II. Healthcare-Specific Culture Challenges

Simply put, the primary mission of the healthcare sector is to save patient lives and keep individuals healthy. To achieve this mission, a healthcare organization must align its cultural priorities in a number of areas—from hiring a sufficient number of doctors and nurses to meet patient needs, to investing in new medical technologies and system infrastructures to support medical operations. Oftentimes, cybersecurity is relegated to a lesser priority or, in some cases, not seen as a priority at all. But emerging technologies are transforming healthcare and surfacing new threats. Failure to mitigate medical cybersecurity vulnerabilities places patients and healthcare organizations at risk of incurring real financial, reputational, and physical harm in the aftermath of a breach, making that healthcare organization unable to achieve its primary mission.

In this section, we explain healthcare's cultural idiosyncrasies to help identify instances where the prevailing culture may directly conflict with beneficial cybersecurity measures and offer policy recommendations on how the two can be reconciled.

i. Diversity of healthcare stakeholders

There exists a diverse ecosystem that includes a range of healthcare organizations with different capacities and practice areas. The healthcare sector simultaneously refers to everything from single physician practices in rural localities to large, multi-state hospital networks with tens of thousands of clinicians. Of the 5,534 registered hospitals in the United States, the majority are

community-run, including nonprofit hospitals (51.48 percent), for-profit hospitals (18.7 percent), and state and local government hospitals (17.28 percent). A small number of hospitals are not considered "community-run" hospitals and are either operated by the federal government (3.78 percent), can be considered non-federal psychiatric hospitals (7.17 percent), or fall into some other category (1.59 percent). Nearly two thirds of community-run hospitals are located in urban centers, with the other third located in rural areas.[64] Given the sheer size and range of players in the healthcare space, cybersecurity policy solutions must be similarly variegated to account for the individual capacities of different providers.

ii. Internal information sharing

The culture of open collaboration in healthcare stems from two places. First, the collaborative information sharing environment is the result of an exploratory and academic community in medicine that encourages teaching and sharing from the outset of a physician's education. A second reason for a collaborative environment is largely practical: in an emergency situation, physicians and nurses must have immediate access to an individual's health information. Some of the most widely discussed cybersecurity challenges that stem from this open and collaborative environment are related to securely sharing patient data and the inherent limits of interoperability in healthcare.

Consider the scenario where an emergency department must administer a certain drug, but is unable to pull up a medical record to see if their patient is allergic to that drug. Or the situation where a patient requires an immediate blood transfusion, but doctors are unable to access the medical records that contain the patient's blood type. In these scenarios, if an emergency department does not have immediate access to the appropriate records and makes the wrong call, a patient could be killed.

In many industries outside of healthcare, cybersecurity professionals are able to restrict access to certain internal systems to only those authorized users who should be able to access that system. This approach is called role-based access control (RBAC). By the same token, multi-factor authentication, a common solution for verifying a user's identity, works hand in hand with RBAC to ensure the right people are accessing the right data. However, in an emergency situation, blocking a nurse's access to medical records with multi-factor authentication or RBAC—for instance, because the patient in question is not in the nurse's typical practice environment—could be a lethal decision. Thus, healthcare providers choose to have an open information sharing environment with few traditional cybersecurity policies in place, which solves the emergency situation problem but introduces another threat: insiders who already have access to a medical record (see *Threat Landscape* section below).

iii. External information sharing

Cybersecurity information sharing between different healthcare organizations, like in many industries, is a complicated and multifaceted challenge. There is a diverse range of healthcare stakeholders with differentiated capacities, and the regulatory environment is sufficiently complex that it becomes difficult to meaningfully share information on emerging threats, such as those affecting new hybrid infrastructures.[65] Furthermore, the amount of information shared across government and industry information sharing organizations is immense, creating a fire hose that is difficult to process, especially for small- and medium-sized healthcare organizations. In short, many organizations, especially smaller and more distinctive ones, are not well served by any of the numerous information sharing and analysis organizations (ISAOs), such as H-ISAC, HITRUST, NIST, and the FBI's Cyber Health Working Group.

iv. Internet of Things (IoT)

There are a number of life-supporting medical devices that can be lethal if misused or compromised following a cyber incident. The devices most vulnerable to attack are so-called legacy medical devices. Legacy medical devices are outdated systems that continue to operate in the clinical setting despite having known cybersecurity vulnerabilities. Academic research and real-world incidents have on countless occasions demonstrated the worrisome consequences of poor medical device cybersecurity in legacy systems, including shutting off life-supporting implanted devices and disabling medical equipment found in operating rooms.[66] On the privacy side, healthcare must also consider how the deployment of these devices creates HIPAA implications due to their role in collecting data—a position that many device manufacturers still shy away from—as well as their network-connected nature.

v. Rapid digitization and interoperability

The healthcare sector frequently discusses how new technologies and data analytics can be used to improve clinical outcomes. As discussed earlier, the proliferation of these technologies, including EHRs and medical IoT, creates a number of cybersecurity vulnerabilities.

Less frequently discussed is how the same types of technologies can be used to protect patient privacy and security. This oversight has led providers to be wary of tools and techniques that could be useful for protecting patients from cyber incidents and slow to adopt them. There is an underlying culture of "no" that has emerged around healthcare cybersecurity technology, which stands in contrast with the often eager adoption of new technologies that promise to directly improve clinical outcomes. For instance, the post-OPM breach report noted the value of an AI-driven solution in mitigating threats, demonstrating that it is time for all industries to embrace these types of tools.[67] Health professionals tend to take an attitude of "if it ain't broke, don't fix it" to cybersecurity, not realizing that their long held methods and tools may actually have been broken the whole

time. While this attitude is beginning to shift in some ways, the industry still needs to take more of a long-term perspective.

If healthcare continues to approach patient privacy and safety in the same way it always has, we risk an even greater number of cybersecurity disruptions that negatively impact clinical outcomes. Viewed through this lens, patient privacy and safety, and therefore cybersecurity, is a patient health concern. With regards to adopting cutting edge cybersecurity technologies in healthcare, there needs to be a shift away from the culture of "no" towards a culture of "yes... and let's be thoughtful about how we introduce new systems." This parallel track of investment and thoughtfulness about how healthcare uses these sophisticated techniques for defending healthcare institutions is important for continuing to deliver the best patient outcomes. It also means investing in healthcare-specific cybersecurity technologies that mesh with the healthcare sector. Going one step further, *any* innovation that is introduced into the healthcare ecosystem must be designed and implemented with cybersecurity as a fundamental priority from the beginning to the end of a technology's life, as espoused by the "privacy by design" or "security by design" principles that have been incorporated into regulations like GDPR.[68],[69]

vi. Personnel

While HIPAA effectively articulates key principles of patient privacy and security, implementation and compliance of these principles often follows rigid check-the-box approaches. This may not lead to effective privacy and security risk management because the checkboxes are unlikely to reflect best practices in risk management and substantial resources are allocated to compliance rather than actually managing risk. A fundamental shift away from the check-the-box approach is required, moving towards HIPAA implementation that is both comprehensive and integrated between privacy and security.

Healthcare organizations vary widely in their security reporting structures, but not so much in the issues they face. Many struggle to designate responsibility and accountability over cybersecurity. CISOs often assume responsibility for cybersecurity matters, but that is not always the case, particularly in smaller organizations that cannot afford dedicated security personnel. Health professionals may not leap at the chance to take on cybersecurity responsibility (even though many continuously interact with sensitive technology) because successful cybersecurity is often seen as avoiding a loss, not making a gain. Without a formal reporting structure, system of metrics that provides basic data on cybersecurity performance, or lead on cybersecurity issues, there is no way to ensure accountability and responsibility.

Exacerbating the issue of responsibility delineation, healthcare systems often silo privacy and security into very different parts of the organization. Privacy usually falls under regulatory-focused legal and compliance teams, while security is

allocated to engineering-focused technical teams. Though they come from different backgrounds and possess very different skills, privacy and security departments share a single mission: to ensure the trustworthiness of patient treatment and data collection systems. It is increasingly apparent that separating healthcare privacy and security teams creates substantial challenges related to privacy and security protections, like long response times, slow evolution of programs, duplication of efforts, and lack of knowledge across silos. Non-healthcare companies, including those in the Fortune 500, less often have this siloed structure and health organizations need not have it either, despite the sector's unique data sharing culture and regulatory environment.

vii. Budget

The healthcare sector writ large operates on margins that are much lower than those of other sectors (2.7 percent in health care,[70] 7.9 percent average across all sectors.[71]) Limited resources, especially within small- and medium-sized entities, make investment into cybersecurity tools and technologies a difficult sell for most nonprofit healthcare organizations.[72] To provide some context, while comparable industries spend about 8 percent of their budgets on structures intended to protect against traditional, external network threats, healthcare organizations generally spend around 1 to at most 5 percent of their budget on this problem.[73] For large organizations with an expansive attack surface, malicious cyber attackers and insiders create persistent threats that are difficult to thwart, even for organizations dedicating substantial resources.[74] Moreover, there is no standard benchmark on the most appropriate allocation of resources for cybersecurity per unit of scale in a health system, making it impossible for providers to weigh the expected margin of return for additional cybersecurity investments. Even non-budgetary benchmarks for cybersecurity systems, like the NIST Cybersecurity Framework[75] or the ISO 27001 standards[76], are difficult to translate into standards that can work specifically for the healthcare sector.[77]

The margin of 2.7 percent in healthcare for FY 2016 represents the average across the entire healthcare sector, which includes both large and small organizations. After disaggregating these groups, the largest healthcare organizations have higher total profits than small-sized healthcare providers (estimated at 6.7 percent), even though margins for patient care still remain slim for both.[78] Small- and medium-sized organizations that are often rural and publicly owned struggle even more than larger organizations because of "dwindling payments, fewer patients, and an inability to compete against larger, better-funded systems when negotiating payment rates with commercial insurers."[79] These already thin margins for small, medium, and large health organizations are only likely to decrease in the future as providers struggle to reconcile rising costs.[80]

While the actual cost of robust cybersecurity programs varies, it does take some resources to get cybersecurity right, and most healthcare organizations think that they do not have adequate resources to implement state of the art monitoring

programs necessary to protect their organizations. Healthcare organizations do have some leeway to make cybersecurity a strategic priority during budgeting season, however it is usually triaged in favor of other interests that are rightfully viewed as more critical (such as hiring additional clinical staff). Still, it is important to find ways to grow the cybersecurity capacity of healthcare organizations, even with the understanding that current budgets and budget priorities do not meet the need.

In one instance that is indicative of the wider problem, a healthcare delivery organization in West Virginia operated with such limited resources that it replaced its vulnerable computer systems only after a massive cyber attack completely corrupted them and shut them down, causing clinical workflow disruption and delay.[81] As technology becomes even more infused in routine healthcare delivery, a cyber attack like the one in this example is likely to be even more catastrophic. This "wait until disaster strikes" approach is not uncommon. Most health systems administrators agree that their security budgets or IT infrastructure would only receive improvements *after* a serious, life threatening incident occurred.[82] Overall, constrained budgets have forced healthcare system to make strategic trade-offs during budgeting processes, and cybersecurity often loses out.

viii. Threat landscape

As with many industries, a challenge for healthcare privacy and security is the insider threat: those people who already have permissible access to a medical record. Insider threats typically fall within the domain handled by privacy teams due to the HIPAA implications of an insider threat. In healthcare, there are two big problems and trends in this regard. First, there are an increasing number of connections and linkages between individuals, healthcare institutions, information exchanges, and interoperable devices, which is incredibly beneficial for providers and patients alike. But simultaneously, there are no controls over who can access those records and devices. For instance, volunteers and first year medical students generally have unfettered access to medical records with virtually no controls in place to stop them from accessing or looking at records. Second, there is generally little risk of someone discovering an unauthorized access, aside from some regular reports or random audits. This is true of nearly every healthcare organization in the United States.

Despite these challenges, healthcare is at an inflection point, presenting numerous opportunities to reshape the culture of the sector according to a more positive and forward thinking vision. The next section describes these opportunities.

III. Healthcare Culture Policy Recommendations

Taken together, the recommendations contained in this chapter set out specific measures needed to shift cultural norms surrounding healthcare cybersecurity. In five years' time, patients should be able to trust providers to protect their personal health information, keep their life supporting devices safe from cyber threats, and continue to deliver uninterrupted healthcare services. The government may be able to help instill this culture through the creation and dissemination of clear security standards and best practice frameworks.[83]

These policy recommendations are directed towards federal agencies including HHS OCR, the Department of Homeland Security (DHS), the Office of the National Coordinator for Health Information Technology (ONC), the Agency for Healthcare Research and Quality (AHRQ), the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), the National Academies, NIST, and others. Recommendations are also directed towards healthcare industry leaders, since the most impactful cultural change may result from a series of normative decisions made by individual providers.

Recommendation #3.1: The Department of Health and Human Services Office for Civil Rights should showcase health systems with innovative privacy and security programs.

Privacy and security teams in the health sector have a hard job. They need to be able to respond to any of a plethora of threats quickly, effectively, and within a complicated regulatory framework, while also building processes and optimizing organizational structure. Healthcare providers need a way to learn about how others have successfully met these challenges. According to behavioral scientists, the best way to spread positive organizational change is through articulating purposeful visions or "stories" for why change should happen.[84] In order to effect change in the culture around healthcare cybersecurity therefore, OCR should utilize the levers at its disposal to tell stories about security role models.[85]

Currently, most of the stories OCR and the rest of HHS tell are cautionary tales about data breaches. As of this writing, the OCR's "Wall of Shame" includes, among many others, a Texas cancer research center that lost two unencrypted USB drives; a South Florida hospital corporation that allowed an attacker to steal data through the login credentials of a former employee; and a global cancer care service that let an attacker access data on over two million individuals, including names, social security numbers, physicians' names, diagnoses, treatments, and insurance information.[86]

We suggest that in addition to the current, more punitive model, the OCR consider adding real world, positive examples of optimal risk assessment

processes. This proposed "Best Practices Showcase" should highlight organizations that are cooperating effectively and thinking ahead about their holistic trust posture, rather than just checking off boxes on security and privacy requirements. The showcase would hopefully put forth forward-looking, health cybersecurity leaders as role models to others in the sector. This approach mirrors best practices in behavioral science, which recommend creating adaptive structures and processes focused on both positive and negative reinforcement.[87] The closest analog to this recommendation currently offered by HHS are the HIPAA case examples, which are woefully unspecific and totally anonymized.[88]

One of OCR's most challenging tasks in promoting positive role models would be to define what constitutes good cybersecurity practices. In doing so, OCR may want to look at how organizations address both privacy and security, in order to promote collaboration and integration between the two domains. It may even want to promote specific privacy-security collaborative activities, such as weekly privacy-security huddles, shared KPIs, and codeveloping risk agendas. The metrics described in Recommendation #3.3 may also help in identifying positive role models.

On top of defining a rubric for what measures quality in this so-called "Best Practices Showcase," HHS should engage in research to find out how to design this program as to be most useful to the industry. Are hospitals interested in this kind of acclaim or do they fear it puts a target on their heads? Do patients consider cybersecurity when selecting a healthcare provider? Are there subsectors of the health system, such as mental health, where providers or patients are more interested in best security practices?

The answers to these questions may reveal that health systems are not interested in contacting OCR and opening themselves up to conversations with regulators. To mitigate this, OCR could start by piloting this program (as the FDA is currently doing with its "Expedited Access Pathway" program for medical devices[89]) in order to take in lessons learned about good processes and insulate both providers and OCR in case this model turns out to be untenable. The program could also focus more on organizations that already have Corrective Action Plans, allowing them to get positive PR for work they have already done and protection from negative PR under nominal OCR experimentation. If needed, OCR could also offer monetary rewards and incentives. In order to facilitate these improvements, it goes without saying that Congress should appropriately fund OCR's essential work, as these budgets have decreased or flatlined in recent years. These budgets could have specific line items for privacy and security education and incentives to ensure the money is spent roughly as outlined above.

By promoting best practices and highlighting institutions that go above and beyond, OCR can hasten the various cultural shifts needed across the healthcare sector to improve cybersecurity. This approach does not require OCR to give

organizations all the answers. Rather, it empowers healthcare organizations directly by amplifying the great work already being done. Recognition is an easy place to start, but monetary rewards could be a possible next step to encourage cultural change.

Recommendation #3.2: Incentivize and provide structures for multi-tiered information sharing for healthcare's diverse practice environments.

Not all healthcare providers have the same cybersecurity needs, and they certainly do not all have the same resources to meet those needs. A large regional IDN hospital might have a CISO and robust security operations center (SOC) in charge of constantly thinking ahead to ward off attacks. A single doctor's practice might only have a sticky note on a computer asking employees not to share passwords. Healthcare professionals need ways to learn, share, and ask questions about the most up to date information on relevant cybersecurity issues. However, the design of these information sharing systems should be specifically tailored to the individual needs of small, medium, and large organizations.

Small organizations, like individual providers, should receive positive incentives for taking basic cybersecurity measures and undergoing education campaigns. The incentives can be modeled after a recent recommendation from AMA, wherein clinicians receive bonus points through the Merit-based Incentive Payment System (MIPS) track of the Medicare Quality Payment Program.[90] As AMA suggests, physicians should be recognized when they used certified and even non-certified health IT, or when they go above and beyond the requirements of HIPAA. To determine the exact criteria, AMA and AHA could leverage their existing relationships and lines of communication with healthcare providers to learn about the cyber needs of their constituents. Then HHS, with input from industry players, could determine the best tools and education solutions to address their issues. Finally, AMA and AHA could once again leverage their existing relationships to communicate and promote those programs back to their constituents. To clear the way for these campaigns, there may need to be regulatory exceptions for cybersecurity products added to the Stark Law and Anti-Kickback Statute (more on this in Recommendation #3.5).

Medium-sized healthcare providers such as individual hospitals or small systems are somewhat caught in an awkward middle, since they may be too large to benefit from basic tips and plug-and-play cybersecurity solutions, but too small to fund a dedicated cybersecurity team that can keep up with the latest developments in the field. To prevent them from falling through the cracks (and building off of the important emphasis of the Cybersecurity Task Force on Managed Security Services), DHS should subsidize their use of managed security service providers (MSSPs), potentially in the form of a tax credit. MSSPs would be able to take some of the burden off of medium-sized healthcare providers from managing their own cybersecurity. In managing multiple organizations, MSSPs

would be able to participate in the cybersecurity information systems aimed at large health organizations.

Large health organizations like IDNs need the most breadth and depth of cybersecurity information. They require real-time knowledge of recent or ongoing attacks, cyber indicators, and threat analysis that provides insights into both external and internal threats with great sophistication. To this end, DHS should support research grants that test innovative approaches pioneered by these large organizations in sharing information through unified analytics platforms that build upon ISAOs and information-sharing groups. Traditionally, this approach has been focused on such grants as those that centered on creating ISAOs and ISACs, but we believe that large health systems themselves might have the most insight into how to pilot local, regional, and ultimately national collaborations. This "laboratory of democracy" approach, as with the states, would complement and overlap with, rather than replace, the very important efforts occuring at the national level. Examples of such collaborations might be interesting experiments about innovation around institutional sharing of SOCs between different health systems, AI-enabled platforms that continuously improve in accuracy as more health systems utilize them, and other high tech and low tech methods of learning from one another.

Recommendation #3.3: Develop the cybersecurity equivalent of the nurse-to-patient ratio.

One of the many key recommendations from the Health Care Cyber Security Task Force report that bears emphasizing and operationalization is that healthcare should consider implementing a "safe patient ratio" for cybersecurity. The core idea behind such a ratio is that in order to guide healthcare providers in their allocation of resources, there should be guidelines for how many team members, or how much budget, should be allocated to cybersecurity, per given unit of scale for a health system. Such a ratio, or basket of ratios, could be similar to the nurse-to-patient ratio mandated by California in 2004.[91]

Simplifying such an elusive and multifaceted concept as cybersecurity into one or a few metrics comes with challenges. The most important step prior to setting a cybersecurity-healthcare ratio is actually to illuminate the factors that go into the numerator and denominator. It may therefore make more sense to say that X dollars must be spent on cybersecurity for every Y patients, or perhaps that one must have A cybersecurity professionals for every B beds at a facility. Many different permutations may exist, but there is not enough data yet to see how well organizations are performing with current cybersecurity resources and what these ratios should be. These high level metrics may be imprecise, but given the pressing cybersecurity challenges described in Chapter 1, more needs to be done to promote a data-driven approach towards cyber resource allocation.

Thus, the first step worth considering is an HHS-mandated and internally shared platform that compiles data on health system size and compares it to budget allocation for security and privacy. Metrics like incidents detected and resolved, budget allocated to cybersecurity, HIPAA complaints received, and more should be broadly provided, perhaps on a trial basis for some subset of thought-leading hospitals.[92] Many of these metrics are already publicly available, such as broad census data on patient flow and bed size, but questions of budgetary spending on cybersecurity or the number of cybersecurity-dedicated team members are more proprietary. Beyond the data needed for a safe patient ratio, this might be a good opportunity to capture information like board reporting structures, presence of certain technologies, and other similar questions.

With this information, it is possible to observe how the scale of organizations, resources allocated, and privacy- and security-related outcomes interact. This information could be used to inform a group like H-ISAC in developing a NIST Cybersecurity Framework specific to the health sector. H-ISAC and the Health Care Industry Cybersecurity Task Force may already have started work on these metrics. In order to provide for the analysis of factors that may contribute to or defend against breaches, de-identified information should also be made available to researchers in the field.[93]

Second, researchers and healthcare industry leaders can determine the appropriate measure that captures cybersecurity resilience in healthcare. A model should be created that forecasts the degree to which the factors affecting healthcare cybersecurity resilience should change according to the scale of an institution. In other words, a cybersecurity ratio. This cybersecurity ratio should take into account a variety of factors (see Table 2) and researchers should continually refine it as new technologies and security practices emerge. Specifically, researchers should develop more comprehensive, quantitative risk assessments based on the strengths and weaknesses of previous ratios, thus enabling a more refined and robust ratio that is constantly evolving.

In order to facilitate these efforts, HHS and other public and private grant-making bodies should set up data-driven challenges and grants to investigate sector-specific factors that lead to an effective (or ineffective) cybersecurity and privacy posture. These grants could take a variety of forms, ranging from competitive federal awards like those administered by HHS and the ONC for information-sharing to national awards for academic research in healthcare like the plethora of programs administered by the AHRQ, the NIH, the CDC, the National Academies, and others. A table of example numerators, denominators, and variables to measure success is provided below.

→ POSSIBLE METRICS FOR CREATING A CYBERSECURITY RATIO

Possible Numerators

- Number of cybersecurity and/or privacy staff
- Money in annual budget for cybersecurity
- Total cybersecurity payroll
- Percentage of budget spent on cybersecurity
- Number and severity of data breaches/cybersecurity incidents
- Patch status of deployed health IT assets

Possible Denominators

- Number of beds
- Number of facilities
- Patients per year
- Revenue

Possible Confounding Variables

- Type of healthcare provider (e.g., community run, federally run, etc.)
- Area of practice
- Physical location of practice
- Usage of specific technologies/devices

Possible Outcome Variables

- Breaches per year

- Events detected/resolved
- Patient satisfaction
- Institutional/cultural knowledge

The overarching result following the establishment of a safe cybersecurity healthcare ratio is the illumination of discrepancies between the recommended and current cybersecurity levels. Organizations will be empowered to identify these gaps and move towards meeting recommended benchmarks.

Recommendation #3.4: Hold boards of directors responsible for healthcare privacy and security.

Cybersecurity is a strategic issue that warrants top level accountability, but not all healthcare organizations give it the requisite high-level attention. Many organizations have CISOs and chief privacy officers who assume authority over security and privacy matters, but outer edges of their responsibilities are often unclear. Without formal reporting structures, oversight for such hairy issues as privacy and security often fall through the cracks and accountability becomes impossible. This oversight can be seriously detrimental to health companies; a high profile cyber attack can bring about irreparable loss of reputation, loss of life, and bankruptcy.[94] But by attending to issues of cybersecurity, a board of directors can signal to the rest of the company that security and privacy should be considerations in any decision from the outset. Even organizations too small or understaffed to have a single person dedicated exclusively to cybersecurity should clearly delineate responsibility.

The Centers for Medicare and Medicaid Services (CMS) can assure substantive board-level representation and minutes-documenting reviews of institutional cybersecurity postures by making them conditions for participation under Medicare. Approaches can be modeled after existing guidance and best practices from compliance programs, but the mechanism by which a cybersecurity lead reports to the board would have to be tailored to the size and structure of each health organization. For instance, this individual might be the CISO and have a literal seat at the table as a strategic member of the board. Alternatively, a smaller institution might have a combined vice president of privacy and security that reports to the audit committee of the board on a quarterly basis. What is important is the independent capacity to raise potential issues and gain visibility at the highest levels of the organization. Therefore, in its requirements the CMS

should not hold health organizations to the unreasonable standard of having zero incidents but instead connect accountability to risk management and the right key performance indicators.[95]

In addition, Congress should consider passing legislation for the healthcare sector modeled after the proposed Cybersecurity Disclosure Act of 2017[96] and New York's Department of Financial Services' first-in-the-nation cybersecurity disclosure regulation[97] to provide guidance on establishing board-level cybersecurity requirements. While the federal bill has not yet passed and the New York regulation could be strengthened by better defining certain baseline risk frameworks upon which to base threat assessments, both highlight the importance of board-level accountability and provide a models for industry and future policy interventions in other sectors, like the healthcare sector.

As a result of such important levers being exercised, healthcare systems would prioritize cybersecurity as a top level objective within their organizations and better security and privacy reporting standards would be implemented across the entire healthcare ecosystem. Existing cybersecurity requirements would be more closely followed leading to fewer exploited vulnerabilities and better responses post-breach. Most importantly, a culture of cybersecurity would be viscerally felt and lived from the highest levels of the organization, and teams responsible for its implementation would feel empowered, energized, and heard in their concerns and suggestions.

Recommendation #3.5: Ease resource sharing regulatory burdens to empower small- and medium-sized organizations.

(Author's Note: On October 10th, 2019, as this paper was going to publication, the authors were delighted to learn that HHS presented a Proposed Rule to update the Stark Law. This Proposed Rule had the goal of spurring value-based care arrangements, but with provisions that also allow for the donation or reduced-cost offering of cybersecurity protections and/or software to affiliated practices from health systems. While it is too early to comment on the implementation of this rule, and the proverbial devil will remain in the details, we are hopeful that this rule is very broadly interpreted to ensure that the wide array of locations between which health data are exchanged are all effectively covered by this exemption, given the significant networked vulnerabilities that exist in our current, highly-interoperable health data ecosystem.)

The Anti-Kickback Statute and the Stark Law prevent health professionals from using their powers of referral for their own gain by broadly regulating the kinds of resources they can share. However, these laws also stymie collaboration in cybersecurity, particularly affecting small and medium practices. For example, under the Anti-Kickback Statute, a large healthcare organization cannot provide a smaller partner with security technology to prevent it from becoming a supply chain liability. Under the same rules, a group of physicians may not be allowed to pool their resources in order to afford a third party cybersecurity provider. Even

free software updates, security education, and technical support from health system technology developers may be illegal.[98]

AMA[99], AHA[100], CHIME[101], HSCC[102], and other organizations have all released letters suggesting cybersecurity exceptions be made to the Anti-Kickback Statute and the Stark Law in response to a Request for Information from the HHS Office of Inspector General (OIG). These exceptions could legally protect cybersecurity best practices and encourage collaboration. Both the Anti-Kickback Statute and the Stark Law have mechanisms by which to allow for benign commercial exceptions. The OIG has the authority to promulgate new Anti-Kickback Statute safe harbors and issue requests for suggestions in that regard every year. The HHS OIG should explore the negative impacts of the Anti-Kickback Statute to see whether it is hindering meaningful industry collaboration on cybersecurity efforts and consider issuing or explicitly requesting comment on a new safe harbor exception for cybersecurity.

Similarly, the CMS has the authority to create new regulatory exceptions under the Stark Law. CMS should leverage this authority to enable meaningful cybersecurity collaboration.[103] Already, both HHS and CMS have created exceptions regarding the donation of EHRs, and a similar approach should be taken with the sharing of cybersecurity resources.[104]

The cybersecurity of small- and medium-sized healthcare organizations are disproportionately impacted by the Anti-Kickback Statute and Stark Law frameworks because they are less likely to have sufficient budgets to run secure practices. Relaxing the regulatory environment would enable meaningful industry collaboration, aiding the security of patients, payers, and providers alike.

Chapter 4: Technology

I. Summary

Most conversations around patient-centered healthcare technology center on leveraging innovations in artificial intelligence, machine learning, big data, natural language processing, and other frontier technologies to improve or enhance clinical outcomes. While these technologies show promise for positively impacting clinical outcomes and, indeed, that should be the primary focus for healthcare providers, there is equal opportunity to consider how these technologies can be applied to improve the cybersecurity of medical devices, patient records, and the overall healthcare infrastructure. Yet, this remains a nascent conversation, even for the most progressive healthcare enterprises. Likewise, although there is a more robust conversation around existing cybersecurity flaws in medical devices and software, little has been done to shore up the technological infrastructure of our nation's healthcare providers.

Indeed, recent ransomware attacks on hospitals have shown how easy it is to bring a health system back to pen and paper. In a recent series of attacks, several hospital systems had their EHR systems rendered inoperable, forcing everyone to use handwritten notes to coordinate care. The true costs in lives and resources of these events are difficult to calculate, but intuitively, that lost insight has a real impact on patient lives.

This is troubling for a number of reasons, especially considering the increasing pace of attempted and successful cyber attacks directed at the healthcare industry in recent years.[105] Unmitigated vulnerabilities create potentially existential medical, financial, and reputational risks for providers. Some of these problems, which are described in more detail in the next section of this chapter, are summarized in the table below.

Table 3: Summary of Healthcare Technology Challenges

Area	Unique Characteristic or Challenge
Legacy technologies	Medical devices and software are often used for a long time. Many have vulnerabilities and do not support patches.
Incident readiness	Even though cybersecurity incidents occur regularly, few healthcare delivery organizations or device manufacturers have plans in place to prevent future cyber attacks.

Area	Unique Characteristic or Challenge
Budget	Limited budgets and tight margins relegate cybersecurity to a secondary priority
Regulatory guidance	OCR's guidance starts with asking that organizations conduct a risk assessment of their environment. That process, however, has been reduced in practice to superficial checklists that leave vulnerabilities unaddressed. There is both a need for health systems to be more creative on this front, as well as OCR to provide more examples.
Small- and medium-sized organizations	Burdensome regulatory environment, just-in-time supply chain, and risk aversion prevent smaller organizations from investing in cybersecurity.
System development life cycle (SDLC) practices	SDLC practices for medical devices tend to be weak and under-regulated, not end-to-end secure.

Despite these problems, the healthcare sector possesses a unique opportunity. Since many organizations have yet to introduce many basic cybersecurity protections and technologies, the sector can "get it right" the first time, rather than trying to reshape an already entrenched cybersecurity infrastructure and culture. Policymakers can encourage a movement towards healthy cybersecurity technology posture in a number of ways:

- Create a government-backed program to encourage the phasing out of legacy technologies and phasing in of secure and interoperable technologies.[106]
- Learn from the financial sector's success in sector-specific cybersecurity investment, spearheaded by National Cybersecurity Center of Excellence.
- Leverage a broad array of existing funding programs to spur healthcare cybersecurity basic research and innovation.
- Create mechanisms for clarifying privacy standards, providing advice, and receiving feedback from health systems, similar to the levels of determination issued by the Internal Revenue Service.

- Strengthen FDA requirements around medical device security, to ensure that security is baked-in at every point in the device's life cycle.

This chapter describes the technological challenges facing the healthcare sector. While this description presents a stark picture of the many challenges facing healthcare, it also foretells the many policymaking opportunities that are borne out of these shortcomings, which are highlighted in the recommendations at the end of the chapter. The range of technologies covered herein is large and includes medical devices (including those that are part of the "medical Internet of Things"), enterprise IT, the cloud and cloud-connected devices, medical device applications and software (perhaps most notably including EHRs), smart building infrastructure, and more.

II. Healthcare-Specific Technology Challenges

The opening statement from the Hippocratic Oath for Connected Medical Devices, a symbolic attestation for the healthcare community crafted by the security and public safety group I Am the Cavalry, reads "New technology introduces new classes of accidents and adversaries that must be anticipated and addressed proactively...The once distinct worlds of patient safety and cyber security have collided."[107] Others have echoed the same sentiment. The June 2017 Health Care Industry Cyber Security Task Force states, "Now more than ever, all health care delivery organizations...have a greater responsibility to secure their systems, medical devices, and patient data."[108] These statements make two similar assertions:

- That even the most promising advancements in medical technology could have an insidious flaw that places patients in harm's way.

- That healthcare providers and policymakers have a responsibility to proactively address these flaws before they are exploited.

We will address these assertions each in turn, first discussing the flaws associated with medical technologies in this section, and next section offering healthcare providers and policymakers recommendations on how to address these flaws.

i. Legacy technologies

Rapid advances in medical device and electronic health technologies have equipped the healthcare sector with a new suite of tools aimed at improving patient outcomes. However, these advancements have created a number of legacy technologies that are vulnerable to cyber exploitation. Legacy technologies are devices and software that are old, outmoded, or outdated in

some fashion, but that are still in use. Due to the length of time these devices and software have been in use, malicious actors and threat researchers have been able to identify a large number of vulnerabilities and exploitable security flaws; at the same time, cybersecurity vendors often provide few modern countermeasures for legacy devices. Exploiting a vulnerability within a legacy technology can lead to "medical device malfunction, disruption of health care services (including treatment interventions), and inappropriate access to patient information."[109] The impact of the 2017 global WannaCry ransomware attack is a stark example of the vulnerability of these legacy technologies.[110]

One factor contributing to the legacy device problem is the lifespan of medical devices, enterprise IT, and systems that house EHRs, which can be used by a healthcare organization for upwards of 15 or 20 years. Old hardware and devices are not necessarily a cybersecurity problem in and of themselves. Rather, the challenge posed by these devices resides in the software they run. The operating systems and off-the-shelf software that undergird these devices have relatively short lifespans, with new versions launched regularly. As new versions are issued, software vendors often discontinue support for previous versions, leaving them largely unpatched and vulnerable. Because newer software rarely finds its way into these systems, outdated medical devices remain in operation, even when the software originally designed to support them have long been discontinued. Further compounding this problem is that devices manufacturers, healthcare providers, and software companies contest who is responsible for identifying, issuing, and implementing security updates.

More often than not, the disclosure of a vulnerability on a legacy medical device is contained in a list of publicly known cybersecurity vulnerabilities known as a Common Vulnerabilities and Exposures (CVE) report. Oftentimes, even after a bug is identified in a legacy system, they do not get patched either because a patch was never issued or it simply was not implemented.[111] CVE reports often include statements to the effect of "there is no patch available to address this vulnerability." In these scenarios, healthcare organizations are left to rely on their existing security infrastructures—such as firewalls and defense in depth models—to protect medical devices from being exploited. However, the security infrastructures that support a healthcare organization's medical devices and enterprise IT systems often fail to adequately reduce risk, as discussed in the next section.

ii. Incident readiness

An independent report from the Ponemon Institute published in May 2017 found that 67 percent of medical device makers and 56 percent of healthcare delivery organizations anticipated that an attack against one or more of their medical devices would occur over the next 12 months.[112] Beyond these troubling forecasts, manufacturers and organizations admitted to past instances where incidents had negatively affected patient health or privacy: 31 percent of device makers and 40

percent of healthcare delivery organizations admitted to being aware of these sorts of incidents. Of those respondents, 38 percent of healthcare delivery organizations said they were "aware of inappropriate therapy/treatment delivered to the patient because of an insecure medical device." Furthermore, "39 percent of device makers confirmed that attackers have taken control of medical devices."[113] These statistics illustrate the worrying number of confirmed incidents affecting patient privacy and the security of care delivery.

Despite the acknowledged risks, the sense of urgency to attenuate the weaknesses found in the medical devices appears to be low: only 17 percent of manufacturers and 15 percent of healthcare delivery organizations are taking significant steps to lessen the impact of future cyber attacks.[114] Outside budgetary restraints, the reasons why organizations are not doing more to improve cybersecurity are complicated. It may be because they are not sufficiently motivated to invest in cybersecurity by negative factors, like cost. Research shows that HIPAA and FDA requirements are surprisingly ineffective at ensuring the privacy and security of medical systems.[115] Or, there may be enough health-specific information in the wealth of proprietary and open source resources for creating effective incident response plans. This paper offers policy to address both reasons.

iii. Budget

Without repeating the extensive conversation on constrained healthcare budgets from Chapter 3, it bears repeating: most health organizations operate on extremely tight budgets. As a result, healthcare leaders are compelled to make tradeoffs during budget planning, which often results in the relegation of cybersecurity to a secondary priority behind such things as hiring additional clinical staff.

iv. Regulatory guidance

This conversation builds on the previous discussion around HIPAA compliance and implementation from Chapter Three - Culture. NIST, HITRUST, OCR, and others have been key in providing guidance to health systems on privacy and security matters related to HIPAA. However, the increasing use of technology across the health system has outpaced the attendant guidance. There was little interaction between technology and the healthcare setting when OCR and others were initially given oversight for HIPAA. Today, however, a huge amount of privacy and security concerns relate to technology. An opportunity thus exists for convening an ever more robust and dynamic discussion about best practices, which should engage all relevant regulators and health systems alike.

Historically, privacy and security risk audits within the healthcare system have only examined random samples or used basic checklists to monitor HIPAA compliance. This approach simply audits the tip of the iceberg, leaving a vast number of records unexamined. Government agencies have not yet embraced

new technologies, like artificial intelligence, to allow for proactive, risk-mitigating privacy and security solutions capable of fully comprehensive audits. A selective and narrow approach leaves such a wide swath of cybersecurity vulnerabilities unchecked that patient privacy and security remain at significant risk.

v. Small- and medium-sized organizations

While small- and medium-sized organizations do not manage the same volume of patient data as their larger counterparts, they still provide vital services that require the collection of sensitive patient information. Further, the highly interconnected healthcare ecosystem means that a single disruption could cause ripple effects that destabilize the industry as a whole. With the introduction of just-in-time supply chain delivery models, for instance, most healthcare delivery organizations operate with "very limited inventories, diagnostic capabilities, or capacity in an emergency, making many healthcare providers sensitive to cascading consequences in the context of a system-level disruption."[116] It is not difficult to imagine a cyber attack impacting a few vulnerable small- and medium-sized organizations, sparking a cascading system-level disruption that is amplified by the limited quantity of inventoried supplies.

Small- and medium-sized healthcare organizations face tremendous difficulties in maintaining a healthy cybersecurity posture. For some small- and medium-sized organizations, investing money to improve cybersecurity capacity is simply perceived as a drain on the bottom line, so they take a chance that nothing bad will happen, often thinking that they are too small to draw negative attention. For other small- and medium-sized organizations, there is often a misperception that implementing security is only achievable through an expensive onboarding of in-house resources, rather than looking to external managed service options that are available to them.[117]

Furthermore, the regulatory environment is perceived by many to be overly burdensome.[118] In particular, many point to existing regulations in the Anti-Kickback Statute and Stark Law[119] that, while important for protecting against fraud and abuse, prohibit the pooling of valuable cybersecurity resources that could benefit small- and medium-sized providers.[120]

vi. System development life cycle practices

When a medical device vulnerability is discovered by a manufacturer or a cybersecurity researcher, healthcare organizations often take one of two actions: either they scramble to apply a patch or conclude (sometimes wrongly) that the impact of the vulnerability to their existing network is minimal. As more and more vulnerabilities are discovered on medical devices, one begins to wonder what type of security practices are performed by actual medical device manufacturers. If medical device manufacturers provide cybersecurity support

for their devices, do these services include security testing[121] from development through end of life? If manufacturers are in compliance with FDA regulations covering medical devices, but fail to implement robust security testing throughout the development life cycle of a product, what does that say about the strength of existing FDA regulations? These are some of the questions that come to mind when discussing the ever-increasing number of medical device vulnerabilities. The answer to those questions vary widely depending on the medical device manufacturer, but studies indicate that it is fairly common to follow weak security standards.

According to the 2017 Ponemon Survey of healthcare organizations and medical device manufacturers, 43 percent of medical device manufacturers do not conduct security tests (35 percent) or are unsure if end-to-end security practices takes place (7 percent) pursuant to an established secure SDLC process during the development of devices.[122] A secure SDLC process is an end-to-end security practice that better ensures device security because it is a *continuous* concern throughout the entire development life cycle, from initial requirements to end-of-life. Even if manufacturers do conduct security tests during device development, only 9 percent of manufacturers say they continue to conduct tests of their medical devices at least annually, a failure in applying effective, end-to-end secure SDLC practices. Healthcare delivery organizations are similar, with 53 percent not testing their devices (45 percent) or unsure if testing occurs (8 percent). While testing is only one phase within the secure SDLC process, this report sheds light on the existing gaps in applying effective, end-to-end secure SDLC practices, as well as the lack of enforcement mechanisms available to government regulators.

Regrettably, this is not surprising. The FDA is the lead government agency tasked with medical device cybersecurity and it has purposefully left cybersecurity regulations vague and largely up to the discretion of medical device manufacturers. According to the FDA, the reason for leaving regulations broad is "because the regulation must apply to so many different types of devices."[123] However, given the high level of medical device vulnerabilities and the admission of poor alignment with established secure SDLC practices, it is clear that the FDA's one-size-fits-all approach has not been successful. It is easy to understand why when reading the existing FDA guidelines, which allow for incredibly loose interpretations of pre- and post-market cybersecurity considerations.[124] FDA guidance and standards do not even require medical device manufacturers to conduct specific (and basic) security tests throughout a product's development life cycle—including static and dynamic application analysis, code review, and penetration tests.[125]

The regulations only require manufacturers to "establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis," which leaves a large amount of discretion up to medical device manufacturers.[126]

Post-market, the FDA provides a series of guidelines for how manufacturers can "implement comprehensive cybersecurity risk management programs and documentation consistent with the Quality System Regulation (21 CFR part 820)."[127] However, these guidelines are also broad, allowing manufacturers to conduct sporadic and self-defined post-market testing that could easily fit within the broad regulatory framework.

It is no wonder that medical device vulnerabilities are so prolific given the fact that the existing regulations do not explicitly require even the most basic cybersecurity testing requirements.[128] Indeed, this is the state of the software and hardware industry writ large, but it should not be the status quo for medical devices given the particular risks to individual wellbeing. Without effective, end-to-end secure SDLC practices incorporated throughout the life cycle of a medical device, design flaws are likely to occur. These flaws could allow unauthorized access, introduce medical risks to patients, and risk the integrity and security of the data generated by a medical device. The reality is that, even with good testing practices, vulnerabilities would still appear at other points in a device's lifecycle. Ensuring end-to-end secure SDLC practices would go a long way in reducing the risks across the entire lifecycle of a device.[129]

Given the myriad challenges around healthcare technologies, including the proliferation of legacy technologies, poor security infrastructures and incident response plans, limited budgets and tight margins, vague privacy and security standards under HIPAA, particular concerns affecting small and medium providers, and weak end-to-end secure SDLC practices for medical devices, it is important for policymakers to take action. The next section details a set of policy recommendations that would empower policymakers do just that.

III. Healthcare Technology Policy Recommendations

The recommendations contained in this chapter focus on identifying technological opportunities and challenges facing the healthcare sector to improve overarching cybersecurity infrastructures and procedures. Together, these recommendations present a vision for the future healthcare cybersecurity tech landscape where legacy medical devices are a thing of the past, new sector-specific cybersecurity technologies are available to all healthcare organizations regardless of size, and regulations and guidance are clear and support comprehensive privacy and security standards that keep patients and data safe.

At the simplest level, these recommendations aim to square the incredible benefits of emerging technologies with the attendant cybersecurity risks they introduce. This means that, in five to ten years, as patients benefit from the incredible advances in artificial intelligence to predict their individual likelihood of getting sick, confidence that their personal information is protected by privacy and security officers equipped with innovative sector-specific tools will also be

possible. Patients will be able to analyze data from their wirelessly connected and implanted medical devices, knowing that those devices were designed with the most robust security testing available and that continuous updates address new vulnerabilities. And healthcare providers will be able to ensure the trustworthiness of their networks so that, even in the face of an internal or external malicious attacker, they can continue delivering immediate, uninterrupted, quality care.

The policies proposed in this chapter are directed towards government agencies including the FDA, the HHS OCR, NIST and its National Cybersecurity Center of Excellence (NCCoE), and DHS, congressional leadership, industry accreditation groups like The Joint Commission (TJC), as well as medical device manufacturers and medical leaders who have influence over institutional policies within the healthcare sector.

It is additionally important to note that the ONC's proposed Trusted Exchange Framework and Common Agreement put these needs in particular focus. These programs offer potential "levers" for setting a higher standard for information exchange, as well as risks if the framework is insufficiently demanding.

Recommendation #4.1: Create a government-backed program to encourage the phasing out of legacy technologies and phasing in of secure and interoperable technologies.

This recommendation builds on the 2017 Task Force Report observation that legacy systems must be secured.[130] To have maximum impact, we recommend focusing on the following more specific recommendations.[131]

With guidance from health care accreditation organizations like TJC, and input from the government agencies (e.g., HHS, ONC, and FDA), Congress should draft an incentive program that seeks to phase out legacy systems, potentially through Medicare and Medicaid reimbursements. The Medicare and Medicaid programs already offer reimbursements and special incentives directly to hospitals for healthcare expenditures. Currently, these programs award a finite amount of money according to a variety of procedural and quality-based outcomes. It is equally important that cybersecurity and privacy outcomes be included in these quality measures since they greatly affect patient safety, dignity, and trust.

Congressional leaders should evaluate incentive options within the Medicare and Medicaid programs to encourage organizations to migrate security services to more trusted, state-of-the-art systems. Since the FDA is responsible for ensuring proper medical device security, they should take the lead in phasing out legacy medical devices. ONC is equipped with the authority to write regulations around the minimum security functionality for EHRs, so they should take the lead in phasing out legacy EHR components. One recommendation from an expert in the field would be to concurrently implement a faster cycle time on security

standards, given the length of time it takes to make a rule. It is important that these efforts be harmonized across agencies since the work of one will greatly impact the other. This push would tie in nicely with the interoperability effort being led by the CMS and would be a great opportunity to incentivize privacy and security as an attendant concern related to interoperability.

Grants, vouchers, and/or tax incentives could be provided to partially offset the costs associated with this transition, with ongoing payments tied to performance and dispersed through a reimbursement mechanism. Any program should be flexible, providing incentives that are tailored to the size and unique needs of each health organization. One way to do this would be to create mechanisms within the Medicaid system, such as demonstration or innovation waivers, that would allow states to experiment with individualized incentive systems. Furthermore, the eligibility of new technologies should be held to a minimum standard of medical device cybersecurity, similar to the provisions outlined in the Internet of Things Cybersecurity Improvement Act of 2017.[132] As a result, the incentives disbursed through the Medicare and Medicaid programs would encourage healthcare providers to purchase new equipment and phase in more interoperable and secure technologies.

Existing programs like the Modernizing Government Technology Act, which created a $500 million fund for updating legacy systems across federal agencies, could also be applied to federal health systems or even expanded to include state and local health organizations.[133] While this program is structured to loan money for capital projects, it could certainly be used to provide resources for health systems that are paid back over time. Another way to hasten this transition is for TJC and the FDA to update their accreditation and regulatory processes to include a cybersecurity interoperability requirement for new technologies.

We acknowledge that the provision of public money to private entities is challenging. But in this particular sector—due to the direct patient safety issues that arise from poor cybersecurity, pervasive budgetary challenges and low margins, the need to (rightfully) prioritize clinical care over investments in cybersecurity—it makes sense to provide these incentives.

Mistakes were previously made when medical devices and EHRs were released into clinics with poor security infrastructures baked-in.[134] In order to avoid repeating a similar mistake when replacing legacy systems, a more robust set of Meaningful Use (now a part of MIPS, under MACRA) requirements articulated in the Certified Health IT Products List (CHPL) is essential. While there was, historically, a challenge with measuring privacy and security efficacy beyond specific EHR requirements in Meaningful Use, we believe that leveraging a risk-based framework to do so is both feasible and essential. There are many stakeholders involved here—health systems, EHR vendors, security vendors, government actors, patients and many more—but a convening and standard setting is necessary. Implementing these solutions would result in the

replacement of unsecure legacy systems with new systems that are both secure and interoperable.

Recommendation #4.2: Learn from the financial sector's success in sector-specific cybersecurity investment, spearheaded by NCCoE.

Cybersecurity challenges across industries are more similar than they are different, but the healthcare sector has many of its own idiosyncrasies. One-size-fits-all solutions often do not work for healthcare because they fail to address the intricacies of HIPAA, issues around sensitive PHI, the contrasting requirements of easy access and strong protection of EHRs, and other factors. For instance, consumer-grade multi-factor authentication (MFA) solutions could catastrophically fail in a Code Blue situation. Caregivers would have no time to input a code from an app or text message to unlock their computer if a patient were literally dying in front of them. Instead, MFA on a clinical workstation must be able to unlock in a fraction of a second, which products currently in the market achieve using biometric scanning or security tokens.

In order to develop cybersecurity solutions tailored to the health sector, the major players should follow relatively successful model of the financial services sector. Large banks with enough liquidity created internal incubators or accelerators that they use to purchase promising cybersecurity companies in order to steer them towards the development of tools tailored for the idiosyncrasies of the financial sector.[135] The benefits of this approach for the finance sector are twofold. First, and obviously, it catalyzes an industry dedicated to developing tools these companies can use in their core businesses. Second, the provision and scaling of these promising companies is a legitimate investment opportunity. If incubated or accelerated companies succeed and gain traction across the financial sector, the bank that invested in them stands to profit. Though the margins in the healthcare sector are, on aggregate, much smaller than those in the fiance, a number of larger healthcare providers have sufficient profit margins to emulate the financial sector model. A few may even be large enough to support this kind of program on their own in internal incubators, like the one Goldman Sachs recently launched.[136]

NIST's NCCoE can serve as a coordinating body to gather the major players of the healthcare industry necessary to form this group of potential investors. The role of government, in this case, should not be to fund or develop the technologies, but to provide information and models for the healthcare sector to take on the task themselves. Sector leaders may benefit from some guidance in conceptualizing the cybersecurity needs of the healthcare sector, and to this end we put forth a three-tier framework:

- *Universal platform technologies*. Tools that assure basic cyber hygiene, including but not limited to coverage from endpoints to data centers, intrusion response and prevention capabilities, and hybrid deployment

options.[137] These are necessary in any industry and are offered by a number of commercial platforms.

- *Industry-specific technologies*. Tools that map onto the unique needs of the health sector, such as EHR privacy monitoring, PHI de-identification, and patient portal security.

- *Subsector-specific technologies*. Tools that are only needed for healthcare providers of certain specialties or sizes. Examples include complex PHI de-identification tools for research institutions, managed service providers for smaller enterprises, and automated IoT monitoring for providers with significant hardware needs.

NCCoE may want to encourage group of industry leaders to focus more on the second and third tiers, since they have the fewest existing industry solutions. NCCoE can further help the industry by increasing how often it publishes guidance on best practices surrounding existing health care technology. NCCoE has already done commendable work in this regard on the second tier—in its guidance on EHRs and picture archiving communication systems—and the third tier—in its analysis of infusion pumps and pacemakers.[138] This work should be scaled up and built upon to address a much wider array of challenges, and guidance priorities should be laid out in a three-year roadmap.

Recommendation #4.3: Leverage a broad array of existing funding programs to spur healthcare cybersecurity basic research and innovation.

In order to keep up with the evolving cyber threats that face the healthcare sector, there must be a paradigm shift regarding current research efforts in healthcare cybersecurity. While a suite of recommendations encouraging additional research is not particularly novel, it bears repeating.[139] Building on the work of the ONC, NIH labs, and the NCCoE, the government should lead the development of an overarching initiative that informs where healthcare cybersecurity may be going in the next five years and future research strategies that could inform that thinking. The first stage of this process should resemble a net assessment, or compilation of active research and development (R&D) efforts aimed at identifying emerging or future threats and opportunities. R&D efforts within this vision could include a focus on securing the cyber-physical vulnerabilities present in connected medical devices and autonomous systems and using emerging technologies like artificial intelligence, big data analytics, quantum cryptography, and blockchain to protect patient data.

Existing funding programs like the Small Business Innovation Research (SBIR) program and the NIH's "R01" standard independent research project grant are important for job creation and innovation. SBIRs are already one of the largest government-industry partnerships with regards to annual budget, but more

needs to be done to focus research efforts in critical need areas like healthcare cybersecurity.

There is growing empirical evidence that government sponsored research projects like SBIRs and R01s are particularly effective at catalyzing innovative projects that would not have otherwise been completed in the absence of funding.[140] Relatively small investments from the government in high tech industries can assist a government up the learning curve and down the cost curve, creating permanent advantages in key industries like healthcare.[141] A supportive policy framework is needed for entrepreneurs and growing firms to bring welfare-enhancing technologies to the healthcare sector. As such, SBIR funding models at the federal and state levels and R01 grants should be expanded to support research specifically in the healthcare cybersecurity field. Policy experiments in other government agencies may provide some guidance on how to develop these funding models.

Policy experiments like the Department of Defense's Fast Tracking SBIR funding model have proven to be particularly effective at aligning departmental goals with an economy in which rapid innovation is rewarded. Fast Track funding increased the effectiveness of SBIRs by encouraging commercialization of specific products and technologies that also met the program's objectives.[142] Increasing SBIR funding for healthcare-specific research that has the potential for commercialization would encourage the rapid innovation and scalability needed to help mitigate the threats facing healthcare.

Beyond monetary investment from the government, SBIRs catalyze further investment from the private sector. SBIRs play a certifying role that can signal to private sector investors that an organization is trusted and worthy of investment. Private investors know that SBIR-funded enterprises have to go through a rigorous application and assessment process. Trust in this process mobilizes further private sector investment in an SBIR company's technology and future commercialization. Without the credibility provided by an SBIR, private investors would be less likely to invest.

Even if an SBIR-funded healthcare cybersecurity business or employee fails or exits the market, there are still gains to be made. The human capital expertise developed through an SBIR-funded research project sticks.[143] Since this expertise can be applied to other companies, it has economic value, especially for the chronically understaffed healthcare cybersecurity workforce. Moreover, there is a huge spillover effect from SBIR funded projects.[144] This means that the net benefits to society stemming from SBIR-funded projects are much greater than projects that do not receive SBIR funding: an 84 percent social rate of return for SBIR-funded projects versus a 25 percent expected rate of return for non-SBIR funded projects.[145]

There are numerous examples where the federal government used tax dollars to invest in R&D projects aimed at meeting specific grand challenges, many of which are comparable to the healthcare cybersecurity vulnerabilities that currently face the nation. For example, the not-for-profit consortium SEMATECH (Semiconductor Manufacturing Technology) was established through an investment from the federal government to address unprecedented challenges in the semiconductor industry.[146] NIST's Advanced Technology Program was created to invest in research projects "that industry on its own could not fully support because of the technical risks involved, and often where timing is critical to eventual economic success in the highly competitive global market."[147] The Partnership for the Next Generation of Vehicles, or "Supercar" initiative, was a partnership between the U.S. government and three automobile manufacturers that sought to create a clean, safe, and affordable car with maximum fuel efficiency.[148]

To best follow these examples, a concentrated R&D effort in health system cybersecurity would need a specific and well-defined problem to address. The exact problem would be determined by the leaders initiative, but three areas of cybersecurity research should be considered:

- *Proactive insider threat detection systems*. One good way to mitigate insider threats is to use AI to flag suspicious, anomalous accesses to patient data. Health systems should ideally have tools to automatically review and document on 100 percent of accesses.[149]

- *IoT medical device security platforms*. As internet-connected medical devices become more prevalent, there must be platforms developed to assure that that they are not only safe from outside attackers but also resilient to component failures, natural disasters, and even collapses in critical infrastructure.

- *AI technology to augment the privacy and security workforce*. Large gaps in the health cybersecurity workforce are in themselves existential threats to the security of health systems. AI tools can be used to mitigate this gap by training models to perform the most rote and mundane aspects of cybersecurity, such as data audits.

Recommendation #4.4: Create mechanisms for clarifying privacy standards, providing advice, and receiving feedback from health systems.

In a recent audit of 166 covered entities, OCR found that only one entity was compliant in their risk management process and none were compliant risk analysis processes.[150] It is unlikely that this abysmal compliance rate is the result of solely of gross negligence in security by health systems. Healthcare providers

may struggle to understand how to comply, especially with certain vaguely defined concepts (such as "security risk"), as providers themselves have suggested. At present, the main mechanisms through which OCR can give guidance are through fines and naming and shaming. These punitive measures may not constitute an actionable precedence for providers in the security measures they are expected to take. Instead, OCR should open up more channels through which it can provide insight to privacy officers.

One way to do this is through more prescriptive standards, but this may compromise OCR's distant position as a regulatory body. A better alternative is to use OCR's power as a convening body to gather a group of experts and stakeholders and have them give definitions and guidance for complying with HIPAA's privacy and security rules. OCR has options for how to create more of a two-way conversation about its guidance: it could convene a regular meeting that may include privacy experts, CISOs, developers, healthcare professionals, and payers; it could hold Q&A conference calls or maintain a helpline for covered entities; or it could maintain more active listservs. OCR need not provide a safe harbor for health systems, only means of consulting.

Offering clear guidance does not preclude using punitive measures. OCR can take guidance from ONC, which has used its extensive regulatory authority over the certification of EHRs to improve their cybersecurity. The American Medical Informatics Association (AMIA) has asked ONC go even further in using this authority to promote security and interoperability measures that would allow for a sort of mass surveillance system to constantly monitor the security of EHRs (not to surveil patients though).[151] OCR should not shy away from wielding its own authority to ensure the compliance with privacy-related HIPAA rules.

These options are not mutually exclusive, although the more hands on approaches may require hiring additional technical experts. If the OCR uses these levers to clarify the privacy standards, it could minimize healthcare provider violations, allow for shared auditing criteria across the health sector, and help CISOs and other privacy and security officers shift time away from mundane auditing tasks and towards meaningful, proactive privacy and security initiatives. An important standard for such work already exists in IRS letters of determination, which provide clarity and comfort to organizations who are innovative and thoughtful, but may still have honest questions on this front.

Recommendation #4.5: Strengthen FDA requirements around medical device security to ensure that security is baked-in at every point in the device's life cycle.

To help address existing gaps in medical device guidance, the FDA should add an additional requirement that ensures device makers use an end-to-end secure system development lifecycle (SDLC). The sheer magnitude of medical device vulnerabilities, coupled with the worrisome reality that most medical device manufacturers and healthcare organizations fail to adequately test medical

devices throughout their development lifecycle, underscores the importance of a renewed regulatory framework. Proper security testing must be ensured throughout the development lifecycle of a medical device. The FDA is well-placed to meet this challenge, with security policy support from agency partners at DHS.

Broadly speaking, the additional requirement would be geared towards implementing secure coding practices and identifying vulnerabilities within medical devices. More specifically, this would include cybersecurity testing best practices such as dynamic and static application analysis after each code change, and penetration testing, among other common cybersecurity measures. In the past, medical device manufacturers have operated with wide discretion over their cybersecurity assessments. According to the FDA, the reason for this loose regulatory standard is "because the regulation must apply to so many different types of devices."[152] The FDA would be wise to provide transitional support through trainings, public outreach, and site visits to help steer manufacturers towards a stronger standard for medical device cybersecurity.

Defining and regulating a secure SDLC process also prevents device manufacturers from "passing the buck" of cybersecurity to health system customers. As previously mentioned, cybersecurity works best when it is baked-in by manufacturers from the beginning and continually reevaluated throughout the development cycle. Health system customers can only wrap security around what has already been built, a method not only far less effective but also one that healthcare systems may not have the technical or workforce capacity to implement.

For example, imagine that an open source software package used in an EHR-connected patient monitoring device is found to have a vulnerability. If the manufacturer designed the device using a secure SDLC, they would be able to update the device remotely and communicate the update to customers. If not, they may have no way to provide a security patch, and the customer, even if they somehow found out about the vulnerability, could at best silo the compromised device from the rest of their network and reconfigure it to work without connecting to an EHR. Even this fix may not be sufficient, and it would certainly not scale to other organizations.

The FDA has already taken some steps towards regulating secure SDLCs. A recent draft guidance they issued includes a requirement for medical devices to provide a "cybersecurity bill of materials," a list of hardware and software components that could potentially become vulnerable. The guidance also differentiates between devices with high security risk, like implanted devices or pacemakers, and standard security risk, like an EHR.[153] These measures are good first steps, but in their current form they only affect devices that require pre-market approval, a class of devices that has been rapidly shrinking over the past few years.[154]

By issuing additional, more explicit guidance on required cybersecurity measures for all medical devices, the FDA can ensure device makers conduct effective security testing practices throughout the development lifecycle of a medical device. In turn, devices will be more secure when they hit the market and will remain secure even after they have been adopted by clinic.

Chapter 5: Workforce

I. Summary

The technical vulnerabilities in healthcare systems are compounded by another challenge: finding people with the necessary cybersecurity skills to protect those systems.

At every conference and closed door gathering of healthcare cybersecurity professionals, one theme is universal: there aren't enough hands to do the work of protecting the modern healthcare enterprise. The workarounds can range from outsourcing huge amounts of work, to building internal training programs from ground zero, to simply telling one's board of directors that an attack is inevitable if they're going to continue to fund at the levels they propose. Frustration is palpable, and answers are few.

The cybersecurity workforce shortage is not unique to the healthcare sector.[155] Globally, the cybersecurity workforce gap is expected to reach 1.8 million by 2022 according to the 2017 Global Information Security Workforce Study.[156] In America alone, employers struggle to fill nearly 200,000 new job openings requiring cybersecurity-related skills each year, including 5,000 information security analyst positions, the most common job in the field.[157]

The workforce gap has led to serious challenges in securing critical public and private data, and the gap is growing. Two schools of thought have arisen to explain this issue. The first posits that the workforce deficit is a function not having enough people in the education pipeline,[158] and policy solutions in this school of thought encourage more students to pursue cybersecurity education programs. The second posits that in addition to an inadequate supply of talent, the cybersecurity workforce lacks mechanisms to match job seekers with job providers.[159] Policy solutions in this the second school of thought aim to better align education and industry, and include efforts to focus education on applied skills, create collaborative opportunities between educators and employers, and improve measurement and communication of employee competencies.

To best ameliorate the problems that fuel the healthcare cybersecurity workforce gap, the community needs solutions that address both schools of thought. Therefore, the policy recommendations in this chapter are divided into two categories: *recruiting*, which largely addresses the first, educational school of thought, and *retention*, which addresses the second, job-alignment school of thought. The two schools are not strictly separated though, and in many recommendations they may overlap. To set the stage for these policy solutions, Part II of this chapter will describe the challenges facing the healthcare sector

that make it particularly sensitive to the cybersecurity workforce shortage. These challenges include:

Table 4: Summary of Healthcare Workforce Challenges

Area	Unique Characteristic or Challenge
Financial limitations	Limited budgets and tight profit margins make it difficult to recruit and retain relatively high-paid cybersecurity talent, especially in competition with other higher-paying tech jobs and flashier defense positions.
Workforce shortage	A shortage of physicians and nurses compels hiring managers to make tradeoffs based on the most pressing hiring priorities.
Skills	Healthcare cybersecurity requires a complex set of hybridized skills.
Job appeal	Healthcare cybersecurity work can appear mundane, time-consuming, and tedious, turning off potential employees and causing existing talent to burn out.
Career paths	Cybersecurity in general has poorly defined career paths and offers limited professional development.
Diversity	A diversity gap in the cybersecurity community writ large limits the pool of available talent, leads to fewer innovations, and introduces troubling social equity concerns.[160]

Part III will then provide specific policy recommendations to meet these challenges, centered on recruiting and retaining top cybersecurity talent. These policy recommendations are:

Policies for Recruiting the Cybersecurity Workforce Needed to Support Healthcare

- Amend the Cybersecurity Enhancement Act of 2014 to incentivize recipients of the CyberCorps Scholarship to serve in specific, critical need sectors like healthcare.

- Under leadership from the U.S. Department of Labor (DOL), HHS, and state and local governments, create and subsidize models for cybersecurity-specific apprenticeships in the healthcare sector.

- Create and incentivize adoption of sector-specific Centers of Academic Excellence designated programs.

- Support an industry-wide approach for creating a healthcare cybersecurity job certification.

- Create a sustainable financing model that supports healthcare providers who typically have the least concentration of cybersecurity expertise.

Policies for Retaining Cybersecurity Professionals in Healthcare

- Provide payroll tax incentives to healthcare providers to address the "brain drain" in healthcare cybersecurity.

- Healthcare leaders should work with security teams when making technical resource decisions that affect a provider's security posture, emphasizing approaches that maximize productivity and reduce burnout.

II. Healthcare-Specific Workforce Challenges

i. Financial limitations

As discussed in Chapter 3, healthcare providers, especially small- and medium-sized organizations, have limited budgets and tight profit margins—a 2.7 percent industry average for healthcare.[161] This limitation makes it difficult to recruit and invest in the development of relatively high-paid cybersecurity talent who often "view an attractive pay package as a given."[162] Operating on a tight margin makes it incredibly difficult to recruit cybersecurity talent who are sought after by higher paying firms in other sectors, like finance and big tech. Similarly, it can be difficult to retain cybersecurity professionals who often leave healthcare to pursue better pay and benefits.[163] This retention problem is referred to as the healthcare cybersecurity "brain drain," which occurs after a cybersecurity manager invests a large amount of time and money into a new hire, only to have an individual leave for another job after a few years.[164]

ii. Workforce shortage

On top of a cybersecurity workforce shortage, most health organizations have a non-cybersecurity workforce shortage as well. Reports from the Health Resources & Services Administration, an agency of HHS, project that there could be a shortfall of nearly 67,000 primary care physicians and a 20 percent shortage of nurses in the United States by 2020.[165] By 2021, there is an expected shortage of 250,000 public health workers. Given competing hiring priorities, healthcare

leaders may, and justifiably so, direct extra funding to attract physicians and nurses rather than cybersecurity professionals. The overarching healthcare workforce shortage combined with limited budgets makes it especially difficult to recruit a robust healthcare cybersecurity workforce.

iii. Skills

Healthcare cybersecurity specialists must not only be equipped with cybersecurity-related skills, they must also be familiar with HIPAA, proper handling of protected health information (PHI), and other healthcare-specific idiosyncrasies. Other sectors face similar challenges and Burning Glass calls these sorts of jobs, which blend cybersecurity technology skills with industry specific expertise, "hybrid jobs."[166] While there is a unique opportunity for job seekers who possess both sets of skills to demand higher salaries, it is difficult to find a single cybersecurity education and training program tailored to the idiosyncrasies of the healthcare privacy and security environment. As such, it is difficult for hiring managers to identify candidates who have all of the necessary competencies required for working in the healthcare setting. These additional requirements make an already scarce set of job skills even more rare.

iv. Job appeal

Potential employees may find healthcare cybersecurity work unappealing, even relative to other mundane cybersecurity work. Currently, many of the daily tasks required of cybersecurity specialists are tedious and involve manually sifting through large data sets, for example checking access logs to ensure that organizations remain HIPAA-compliant. While privacy and security teams are often artificially separated, sometimes, during security and/or privacy audits access logs must be analyzed to identify HIPAA violations. To complete this task, healthcare workers may first print access logs, which are documents that have tracked the digital behavior of specific employees. As healthcare employees interact with dozens of patients every day, access logs can be dizzyingly long. After printing or exporting a log to Excel, it is not uncommon for a cybersecurity analyst to go through every single line of data, using a highlighter to flag instances where a colleague may have improperly accessed a patient file.[167] Compared to flashy national security and intelligence positions in the Department of Defense, it is no wonder that healthcare cybersecurity work can appear unappealing.

Healthcare security work can be so uninteresting and unrelenting that professionals may burnout and leave the industry altogether. Generally speaking, information and cybersecurity teams in healthcare are small and compete with other core staff departments for limited funding. This means that security teams are typically understaffed and under-resourced, creating more stress for current employees. Keeping cybersecurity specialists isolated, sifting through security reports in a small backroom leads quickly to burnout. A white paper by social

scientist Andrea Little Limbago found that burnout was one of the three main challenges to retention in the tech industry as a whole, alongside poorly defined career paths and non-inclusive culture (discussed in the next two sections)[168].

v. Career paths

There is no often traveled single path to becoming a cybersecurity professional, and professionals come from all different backgrounds. According to one study, 87 percent of today's global cybersecurity workforce did not start out in cybersecurity, and 30 percent did not even come from an engineering or IT background.[169] As receptive as this seems on its face, the lack of clear paths means that people interested in cybersecurity may not know how best to gain skills and find a job. Indeed, the same study found that 31 percent of global hiring managers in cybersecurity believed that the absence of a clear information security career path was an important factor in why they could not hire enough people.[170]

Poorly defined career paths and lack of professional development also lead many existing security specialists to exit the profession. According to Matthew Doan, a New America cybersecurity fellow and senior associate at Booz Allen, there is a dearth of opportunities for cybersecurity professionals across industries to move both vertically and laterally throughout their career. In healthcare, cybersecurity specialists similarly lack well-defined career paths and professional development opportunities.

vi. Diversity

The diversity problem within the broader cybersecurity workforce exacerbates the workforce challenges presented here. An (ISC)2 study from March 2018 found that, although minority participation in the cybersecurity workforce is higher (26 percent) than the overall U.S. minority workforce (21 percent), there are still pay discrepancies and promotional barriers that disproportionately affect people of color, and in particular women of color.[171] The study found that more minorities in cybersecurity have obtained a master's degree or higher (62 percent) when compared to their white counterparts (50 percent), yet minorities are still paid less on average ($115,000 for minorities, compared to $122,000 for the overall cybersecurity workforce) and promoted less often (23 percent of minority cybersecurity professionals hold a role of director or above, compared to 30 percent of their Caucasian peers). Female participation rates are also dismally low at only 14 percent of the cybersecurity workforce in North America.[172]

In many ways, these statistics illustrate that the cybersecurity workforce is dominated predominately by white men. This diversity gap is problematic for three reasons. First, lack of participation, especially among women, limits the pool of available talent in the workforce. Second, homogenous teams produce less innovative work.[173] And third, there is a troubling social equity problem when

minorities are not afforded the full pay and promotional opportunities stemming from relatively high paying cybersecurity jobs.

Beyond this broad culture of discrimination, it is hard to pinpoint a unique culture of discrimination specific to the healthcare sector. Still, healthcare-specific cultural factors do influence employee turnover. In particular, the healthcare sector is extremely slow to embrace new technologies that could enhance and support employee's work; for example, the vast majority of the healthcare sector used paper records until 2009. The sector adopted electronic health records only after a massive government incentives program sparked this transition. The conservative, tech-wary culture in healthcare can restrict the adoption of security tools and technologies that would support the cybersecurity workforce.

These challenges are situated within the problematic national cybersecurity landscape, where progress is painfully slow and policymakers remain lukewarm towards concrete cybersecurity action (or even draft counterproductive policies), all while cybersecurity incidents continue happening at an accelerated clip. Such realities make the healthcare cybersecurity workforce shortage especially difficult to solve. In order to ensure the secure and uninterrupted provision of healthcare services, this report presents a comprehensive healthcare cybersecurity workforce vision as a guide for community stakeholders including healthcare industry leaders, federal, state, and local policymakers, and academic institutions.

III. Healthcare Workforce Policy Recommendations

This report offers a healthcare cybersecurity workforce vision built on the following two pillars:

- Recruiting a diverse workforce that is well prepared for healthcare-specific cybersecurity challenges.

- Retaining cybersecurity professionals within the healthcare sector.

In short, the aim of this vision is to create a more robust healthcare cybersecurity workforce backed by sector-specific job training programs and technologies. Necessarily, a robust workforce will more accurately reflect the population it serves and add value to security outcomes through increased workforce diversity. Moreover, solutions will draw upon a dual approach that emphasizes both A) expanding educational offerings that attract more students to the healthcare sector and B) creating a better system for matching healthcare cybersecurity job seekers with hospitals and other healthcare providers. While the specific recommendations contained in this report are geared specifically towards

addressing the healthcare cybersecurity workforce gap, the two pillar model above is broad enough to prove useful for other industries seeking to address their particular cybersecurity workforce challenges.

Recommendations for Recruiting the Cybersecurity Workforce

Recommendation #5.1: Amend the Cybersecurity Enhancement Act of 2014 to incentivize recipients of the CyberCorps Scholarship to serve in specific, critical need sectors like healthcare.

One of the key programs that seeks to expand the cybersecurity talent pipeline is the CyberCorps: Scholarship for Service program, administered by the National Science Foundation in coordination with the Office of Personnel Management and the Department of Homeland Security. Established in 2000, the CyberCorps Scholarship provides tuition and a stipend to students in return for a dedicated term of service in a federal, state, local, tribal, or territorial government organization. The obligation for government service requires that a scholarship recipient serve in a qualifying position for a period of time equal to the length of the scholarship, so generally between one and four years.

Considering that only about 3,300 students have completed the CyberCorps Scholarship program since its establishment in 2000, it is difficult to assess its impact on the cybersecurity workforce beyond the simple observation that CyberCorps has not significantly narrowed the gap.[174] While future independent assessments should be conducted to fully understand its effects, research will likely show that the program has an even lesser effect on the healthcare cybersecurity workforce. There are several reasons to suggest that CyberCorps fails to perceptibly improve the healthcare cybersecurity workforce.

First, the obligation to serve in a government agency precludes most healthcare providers from eligibility. According to the American Hospital Association's 2018 Hospital Statistics, there are 5,534 registered hospitals in the United States.[175] Of these, nearly 80 percent of hospitals are privately owned, either as not-for-profit or as for-profit community hospitals. Only 956 hospitals are owned by state and local governments and even fewer, 209, are federally owned. With so few government-owned hospitals, it can be difficult for CyberCorps Scholarship recipients to find eligible government healthcare operators that appeal to them. Thus, since most healthcare organizations are privately-owned, cybersecurity professionals supported through the CyberCorps Scholarship program have limited options to start their careers in the healthcare sector—or any other critical private sector, for that matter.

A second reason CyberCorps will not lead to significant changes in the healthcare sector is that, even for those individuals who choose to enter one of the few government-owned healthcare organizations, the required term of service is too short to guarantee that individuals will remain in the healthcare sector for more than a few years. Cybersecurity professionals who complete the scholarship

program are likely to feel drawn to other fields outside of healthcare. As detailed above, healthcare struggles to retain cybersecurity talent more than other fields.

Given these weaknesses, the current CyberCorps model is unlikely to significantly move the needle in addressing the healthcare cybersecurity workforce shortage. Still, recognizing that relatively small changes to the program could address its shortcomings and help narrow the gap in one of America's most fundamental critical infrastructures, the Cybersecurity Enhancement Act of 2014 should be amended to incentivize recipients of the CyberCorps Scholarship to serve in specific, critical need sectors like healthcare. The *Cyber Scholarship Opportunities Act* (S. 754) recently introduced in the Senate and unanimously approved by the Senate Committee on Commerce, Science, and Transportation, may help do that.[176]

Importantly, this bill would allow CyberCorps Scholarship recipients to fulfill their post-award service obligation outside of strictly government-run organizations; specifically, they would be allowed to work in a "nonprofit that is considered to be critical infrastructure."[177] This new provision encompasses nearly 60 percent (or 2,849) of community owned hospitals that, for the first time, would be eligible organizations for the post-award service obligation. While this still leaves over 1,000 investor owned (for-profit) community hospitals ineligible under the CyberCorps program, the shift to include nonprofit critical infrastructures is a significant improvement.

Since the aim of this provision is to support the beleaguered system of critical national infrastructures, and healthcare is one of the most critical need sectors, it makes sense to specifically name healthcare in the text of the bill and provide extra incentives to individuals who choose to fulfill their service in a qualifying healthcare position. Considering the fact that cybersecurity threats fail to discriminate between for-profit and nonprofit entities, lawmakers should also weigh the merits of allowing post-award employment obligations to be fulfilled in for-profit healthcare organizations.

Recommendation #5.2: The US Department of Labor, HHS, and State and Local governments should enable models for cybersecurity apprenticeships in the healthcare sector.

Alongside the DOL, HHS has recognized the importance of developing general information technology apprenticeship programs[178] in the healthcare sector. This includes a recognition of apprenticeable occupations like information assurance specialists, information and IT project managers, and IT generalists.[179] However, the current focus on providing federal, state, and local funds for the development of health IT apprenticeships leaves notably absent an apprenticeship model focused specifically on developing the healthcare cyber*security* workforce. While there is a temptation to rely on industry to lead the development of apprenticeship programs,[180] the only way to achieve scale is through a systems-

level approach that partners public and private entities through deliberate policy-grounded decisions.[181] These policy decisions can take a number of forms.

First, policymakers should outline a clear framework that establishes healthcare cybersecurity apprenticeship program requirements, including general guidance on the roles and responsibilities of the healthcare sector, apprenticeship intermediaries,[182] and the education system. It is important to be clear that this recommendation calls simply for a standards framework, rather than a strict set of regulatory requirements. The registered apprenticeships program requirements from the DOL serve as a good model to achieve clarity, but state and local policymakers can codify their own healthcare cybersecurity apprenticeship program standards framework. Since around half of the states already follow their own apprenticeship registration models that are different than the federal DOL registered apprenticeships program, this is particularly applicable. Important in this regard is first identifying and standardizing the core competencies of a "healthcare cybersecurity expert." This task may be best coordinated through NIST's National Cybersecurity Center of Excellence (NCCoE). NCCoE is well-equipped to convene the range of healthcare stakeholders necessary to create such a standard, including healthcare industry representatives, educational programs including apprenticeship providers and intermediaries, academic institutions, and relevant public-sector entities.

Second, federal and state policymakers should incentivize industry groups and apprenticeship intermediaries to create cybersecurity-specific apprenticeship programs in the healthcare sector. While some healthcare providers may be comfortable with existing health-IT apprenticeship models, healthcare cybersecurity apprenticeships will be foreign for most (if not all). To ease a transition and incentivize employers to start and run a program, action at the federal and state level must invest in apprenticeship intermediaries, marketing, and research. These incentives can be constructed in a number of ways, either through subsidies provided directly to employers, tax breaks, or public service agreements similar to the CyberCorps Scholarship.[183]

For a number of reasons, apprenticeships in the healthcare sector are particularly effective at addressing recruitment and retention issues. First, healthcare apprentices have a clearly defined career path with upward lattices, making it more likely that they will stay in their job longer.[184] Second, the "earn while you learn" model instills a sense of loyalty within healthcare employees who feel invested in by their organization, thus increasing retention. Third, apprenticeships have a built-in mentorship component that is critical not just for training, but also for retaining new hires, especially those who come from diverse backgrounds. In the end, healthcare organizations that incorporate apprenticeship training models improve patient care, cultivate a diverse workforce that more closely resembles the patients being served, and cut costs associated with employee turnover.[185]

However clear the benefits of these healthcare apprenticeship models, federal, state, and local authorities are still in the early stages of adopting even the most basic cybersecurity apprenticeship models,[186] so conversations about hybrid, healthcare-specific cybersecurity apprenticeships are still a long way off.

Nonetheless, as more state and local programs opt to develop healthcare cybersecurity apprenticeship programs, they should learn lessons from successful models in other, non-cybersecurity related healthcare occupations. A distance learning option, for example, is especially beneficial for individuals seeking a healthcare cybersecurity apprenticeship since much of the work can be done remotely, it maximizes flexibility, and rural healthcare providers can recruit talent from the outside.[187]

Finally, when enabling healthcare cybersecurity apprenticeship programs an important distinction must be made between the healthcare IT apprenticeships that exist in some density and the healthcare cybersecurity apprenticeships that are especially rare. While healthcare IT apprenticeships help to fill the anemic health IT workforce, this does not directly address the shortage of cyber and information security (IS) professionals in healthcare. In their analysis of healthcare cybersecurity and cyber threats, authors Aurore Le Bris and Walid El Asri noted the flaws in conflating cybersecurity occupations (they use the term information security, which falls under the cybersecurity umbrella) with information technology occupations:

When the hospital does have an IS staff, an improper organizational structure may prevent them from having the sufficient leverage to define strong security policies. In fact... the Information Security team is most often integrated into the IT department and so under the control of the CIO. However, IS and IT have diverging guidelines: IT aims first at making systems easy-to-use whereas IS aims at making them secure - that can increase their complexity for users (e.g. 2-factor authentication). As a result, in conflictual situations, IS considerations tend to be discarded in favor of the IT ones.[188]

It is important to separate information *technology* from *cybersecurity* since the related occupations should manage different areas of work while still working in cooperation with each other.[189]

Recommendation #5.3: Create and incentivize adoption of sector-specific Centers of Academic Excellence (CAE) designated programs.

With input from HHS, NIST, industry leaders, and academia, DHS and the National Security Agency (NSA) should create sector-specific CAE[190] designations to incentivize and reward higher education institutions that create cybersecurity programs related to critical infrastructures, particularly healthcare. There is precedent for differentiating between various CAE programs, for instance the CAE-CD (Cyber Defense) and CAE-CO (Cyber Operations)

programs are two existing variants that can provide a framework for further sector-specific differentiation. Creating a healthcare CAE designation will encourage higher education institutions to create new programs specifically designed to train students in the idiosyncrasies of healthcare cybersecurity. This designation will supplement the expansion of academic specializations that could support cybersecurity apprenticeships and cater to those students who either prefer completing their postsecondary education before entering the workforce or want to transition into a different career.

Receiving CAE designation is based on a broad set of criteria, meaning there are no sector-specific requirements for this designation. Without sector-specific requirements for CAE designation, the trend is for educational institutions to create broad cybersecurity programs that train cybersecurity generalists. For specialized critical national infrastructures like healthcare, with idiosyncratic data, privacy laws, and cyber threats, having programs with a more nuanced curriculum would be helpful. Creating sub-specialties within a generalized program may also be an appealing approach.

While institutions may begin creating such sector-specific programs out of a desire to have a competitive advantage over other schools, Congress can incentivize action. At the most basic level, funding for general research into the best practices of sector-specific education programs would be a valuable contribution. NSF's Secure and Trustworthy Cyberspace (SaTC) program serves as a good model for this sort of research, but research outcomes covering education will be limited since funding is capped at $300,000 and the maximum funding duration is two years.[191] In parallel to this research effort on best practices in cybersecurity education, Congress should provide increased funding to centers who earn the proposed healthcare CAE designation presented above. As a result, even more institutions would create certified cybersecurity instructional programs related to healthcare and more students would be equipped with the hybridized skills required to serve as healthcare cybersecurity specialists.

Recommendation #5.4: Support an industry-wide approach for creating a healthcare cybersecurity certification.

NIST, through the NCCoE, should leverage its convening power to bring together relevant stakeholders who can help inform the standards needed in a healthcare cybersecurity certification.[192] These stakeholders include industry associations like CompTIA, training providers like SANS Institute, professional organizations like the International Association of Privacy Professionals, International Information Security Certification Consortium, hiring managers, and healthcare industry leaders.

However useful it may be to quickly identify an individual's skill sets using an industry certification, and whatever the benefits for job advancement, obtaining

a certification can be difficult and is not the only way to demonstrate capability. For example, attempting certain tests can cost an individual anywhere between $330[193] and $2,300,[194] with required renewals costing an additional fee. Certifications may also depend on demonstrated work experience of four or five years for full certification,[195] a prohibitive barrier for newcomers with no formal work experience. Given that the cybersecurity profession is one deeply tied to the expertise of hackers and self-taught professionals who often acquire skills outside of the traditional workforce and education systems, requiring work experience as a prerequisite to certification may be a barrier to entry for some otherwise qualified individuals.[196] Formal work experience may be unnecessary if an individual can demonstrate competency during a boot camp, capture the flag competition, non-traditional training program, or during a hiring simulation exercise.

While there are certifications available for less experienced candidates or for those who obtain skills outside of formal employment, these "entry level" certifications do not tend to land people jobs at the same rate as the certifications that require work experience. The problem here is that employers do not offer jobs that match with entry level certifications. Thus, despite all their benefits in ensuring industry standards, the mismatch between entry level certifications and available jobs accepting them restricts the number of available pathways into the industry. Given these drawbacks, one may wonder if creating a distinct certification for healthcare cybersecurity is a wise course of action. Indeed, it can be, so long as a number of factors are met.[197]

First, the certification must ensure that employees not only possess generally transferable cybersecurity skills, they must also understand healthcare-specific cybersecurity nuances. These nuances include regulations around data security and privacy stemming from HIPAA, handling PHI, protecting patient flows, tracking insider threats, and understanding the culture of healthcare that makes access control different from other industries.

Second, there must be a suite of certifications that covers the spectrum of junior and senior employees. Going a step further, there must be industry alignment to ensure that employers will actually buy into the value of entry level certificates, in particular. In other words, certifications should not be viewed primarily as "career escalators" that position an already established cybersecurity professional for upward mobility.[198] Rather, efforts should focus on certificates that serve as "door openers," which create new opportunities for more people to enter into the healthcare cybersecurity labor market. To achieve this, it may also be necessary to better align the incentives of certifying authorities to those of their job seeking test takers. By fostering this sort of industry-wide approach, more avenues for entering the healthcare cybersecurity workforce will open while still ensuring employee competency.

Finally, in recognition of the "door opener" approach to certification, employers must accept the need for jobs that are doable by workers with fewer than five years of work experience. This elevates the importance of in-house career development and mentorship programs. Human resource teams within healthcare organizations will need to lead the development of these programs and create specific mentorship initiatives for diverse hires.

Recommendation #5.5: Create a sustainable financing model that supports healthcare providers who typically have the least concentration of cybersecurity expertise.

To address retention challenges at rural and small/medium-sized organizations, the federal government should consider a model similar to the National Health Service Corps or the Indian Health Services program, designed to attract cybersecurity experts to rural healthcare providers where it is least concentrated. State and local governments can also prioritize subsidies associated with an employee moving from a higher paying job to a lower paying one and cover relocation expenses to a rural community.

Many small- and medium-sized healthcare organizations still rely on local servers and databases stored in-house, "often in closets or in unsecure infrastructure."[199] There is a great opportunity for healthcare to shift to hosted, cloud, and shared computer environments, but the continued reliance on local servers and in-house databases is likely to persist for some time given the capital investment limitations and the conservative tech postures of most small- and medium-sized organizations. The mentality that tech infrastructure should be stored in-house is the same mentality that leads many healthcare providers to think that they must have physically present, in-house cybersecurity staff (rather than contracting someone to work remotely). For some healthcare providers, where servers and databases require a physical connection for access, this does make sense. And until healthcare providers make the physical and mental transition to embrace hosted, cloud, or shared computer environments, cybersecurity professionals will be called to all corners of the country to fill positions in the rural locations. These positions can be especially difficult to fill because of their isolated location and lower pay.

The National Health Service Corp and Indian Health Services provide full or partial federal support either through direct grants or loan repayment programs for medical students who agree to work in underserved, typically rural communities. These programs grew from the recognition that rural communities faced an even more pronounced challenge in attracting and retaining medical doctors. The same difficulty presents itself for attracting cybersecurity professionals. Small- and medium-sized healthcare organizations in rural locations have a pronounced lack of cybersecurity expertise at their disposal. This shortfall makes it difficult for small- and medium-sized organizations to maintain strong security postures.

Recommendations for Retaining Cybersecurity Professionals

Considering the shortfall of cybersecurity talent in healthcare, it is promising to see hiring managers already prioritize recruiting cybersecurity professionals. The Global Information Security Workforce Study noted that healthcare is expected to expand its cybersecurity staff more than any other industry, with 39 percent of hiring managers expecting to increase their cybersecurity workforce by 15 percent or more in the next year.[200] This "more butts in seats" approach is an important part of the strategy for shoring up the healthcare cybersecurity workforce. However, while much of the cybersecurity workforce conversation is rightly focused on recruiting more talent, an equally important conversation is on how to retain cybersecurity specialists in order to ensure that the field does not leak talent and face a perpetual shortage.

Recommendation #5.6: Provide payroll tax incentives to healthcare providers to address the "brain drain" in healthcare cybersecurity.

To counteract cybersecurity "brain drain"in healthcare and other critical infrastructures, the federal government through Congress should create payroll tax incentives for companies in chronically understaffed, high-need sectors like healthcare. While federal tax dollars may move the national needle most effectively, states can leverage their economic development resources to encourage similar movement in their local health sectors. There are many examples of federal tax incentives and credits being used to stimulate and support certain industries and occupations, including as part of the American Recovery and Reinvestment Act of 2009, the 2010 Hiring Incentives to Restore Act, and the recent Tax Cuts and Jobs Act approved by Congress in December 2017. The most helpful tactic for encouraging retention of healthcare cybersecurity professionals would be a payroll tax incentive that rewards healthcare providers for having long-serving cybersecurity employees. Several requirements could be included in a tax incentives plan to help reach this goal.

First, a healthcare provider should be required to employ the same person in a cybersecurity-related position for a minimum number of years. Second, after this requirement has been met, providers would become eligible for a payroll tax benefit. Third, as an added incentive for even greater retention, benefits could increase over time as employees remain in their positions. In other words, the longer a healthcare provider employs the same individual in a cybersecurity job, the higher the payroll tax benefit granted to that provider.

Together, these requirements would create an structure whereby healthcare providers are incentivized to to retain their cybersecurity staff for the maximum amount of time possible. In order to do so, providers would need to offer more competitive salaries, bonuses, and professional development opportunities, making them more competitive in the labor market.

Recommendation #5.7: Empower employees with artificial intelligence and automation tools for time- and data-intensive tasks in order to maximize productivity and reduce burnout.

Healthcare leaders should empower current cybersecurity professionals with tools and technologies to support employees whose workflows are repetitive, involve large amounts of data, or require fast responses. The mundane and time consuming task of manually auditing patient logs to check for HIPAA compliance is a good example of a task that could be eased and improved through the use of machine learning tools. Not only is this process a pain for the employee tasked with the audit, it also presents a patient privacy and safety issue. Since a manual audit requires a significant amount of time and data, it is nearly impossible for a cybersecurity professional to conduct a fully comprehensive security audit of every patient record and connected medical device. This means that some exploited vulnerabilities could remain unaddressed for months or even years.[201] Tasks like this one are optimal use cases for artificial intelligence tools.

To maximize productivity and reduce burnout, healthcare organizations should adapt their institutional policies to focus on technologies that can automate time-intensive tasks and allow for efficient review of large patient data sets. Leveraging these technologies would allow cybersecurity professionals to focus more of their time on other more challenging and interesting organizational priorities like investigating incidents, creating high level strategic plans for better security training and incident response, cyber hygiene, and HIPAA compliance training. Boredom and stagnation contribute to employee turnover.[202] By reducing the amount of time spent on mundane tasks and increasing opportunities to engage in higher level thinking, healthcare providers are more likely to retain employees.

Chapter 6: Conclusion

This report is a call to arms. Our framing of healthcare cybersecurity as a patient safety issues is by no means new. But it is certainly not the industry standard either, and for the reasons we have seen, it deserves to be. That needs to change, because when envisioning the state of healthcare cybersecurity in five years time without that reframing, the worst case scenario is so striking that it is easy to fall into pessimism. In this world, attackers become so proficient and so prodigious that hospitals include ransomware payments as part of their annual budget. Patients withhold critical information in fear of data breaches and refuse lifesaving medical devices in fear of horror stories they have heard about hackers taking over pacemakers. Old, unpatchable medical devices are used every day, while the few new devices sit in near-mint condition, waiting for security professionals to make sure they won't introduce yet another vulnerability. Approval takes a long time anyway, because turnover of security workers is high. Experienced healthcare security professionals get so bored going through logs and dealing with compliance issues that they quit in frustration. Few candidates are there to take their place—any job seeker that learns of the healthcare sector's low pay and arcane regulatory environment quickly flees to greener pastures.

This image is so visceral (and so close to what we hear from so many frustrated healthcare CIOs) that it almost feels real. But we are optimists. With a change in the narrative toward one that emphasises the patient safety dimension supported by the timely implementation of the sort of recommendations we have outlined in this report, we can imagine a much rosier healthcare cybersecurity landscape. Here, healthcare providers big and small, urban and rural, understand their privacy and security concerns and know how to address them. Organizations pool security resources for mutual benefit and advise one another through new information sharing channels. HIPAA is no longer mysterious and fear-inspiring. Rather, providers usually understand what best practices look like, and when they do not, they know where to ask questions.

In this scenario, the old, tan-colored, vulnerability-ridden medical devices have been swapped for top of the line IoT devices, all with the hard-earned FDA cybersecurity Software Development Life Cycle seal of approval. An investment boom has led to a surge of innovation in the sector and cybersecurity is at the forefront, with blockchain-based EHR systems for file integrity, real time network analytics that leverage automated incident response playbooks, and AI for insider threat detection.

Here, cybersecurity workers are no longer isolated from the rest of the organization. They are an integral part of overall strategy and are accountable to the board of directors, who receive regular updates on their work. Recruitment is easier because certification programs and Centers of Academic Excellence have created new talent pipelines. Employees that are hired stay on for longer because

they have ample opportunities for growth and automation tools help them avoid the tedious aspects of cybersecurity work.

With the right interventions from the government and the private sector, this second, more optimistic vision can be realized. These interventions are not all easy wins. They involve multiple governmental bodies, several industry organizations, and the sixteen million people working in the healthcare sector today.[203] However, by following the cultural, technological, and workforce recommendations made in this paper, patients five years from now will enjoy better security, better privacy, and therefore better health outcomes.

Appendix: Summary of Policy Recommendations

Culture

Recommendation #3.1: The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) should showcase health systems with innovative privacy and security programs.

> Rather than a punitive "Wall of Shame" philosophy that focuses on data breaches and the failures around them, OCR should emphasize positive examples of risk assessment and thinking holistically about trust. This can empower healthcare organizers by emphasizing the positive work already being done in privacy and security.

Recommendation #3.2: Provide multi-tiered information sharing for healthcare's diverse practice environments.

> Small, medium, and large providers have different needs and different capacities when it comes to addressing the privacy and security challenges of today's healthcare sector. The American Medical Association, American Hospital Association, HHS, and other organizations should work to design information sharing systems specific to these varied needs and capacities.

Recommendation #3.3: Develop the cybersecurity equivalent of the nurse-to-patient ratio.

> To guide the allocation of cybersecurity resources within health organizations, setting benchmark ratios for budget, team members, and other factors can assist organizations with less clarity on how to quantify their cybersecurity. Because of the difficulties inherent in picking metrics, HHS and other grant-making bodies should spearhead data collection to inform the design of this ratio.

Recommendation #3.4: Hold boards of directors responsible for healthcare privacy and security.

> Formal reporting structures for privacy and security incidents are essential to effective oversight, and this extends to receiving top-level support from the board. Congress, through legislation, and the Centers

for Medicare and Medicaid Services, through its conditions for participation, can encourage or require board engagement with privacy and security issues at each provider.

Recommendation #3.5: Ease resource sharing regulatory burdens to empower small- and medium-sized organizations.

The Anti-Kickback Statute and the Stark Law prevent health professionals from using their power of referral for their own gain, yet they also limit collaboration on cybersecurity issues. HHS and CMS should thus create regulatory exemptions that allow for cybersecurity collaboration under these laws, which will particularly benefit small- and medium-sized organizations.

Technology

Recommendation #4.1: Create a government-backed program to encourage the phasing out of legacy technologies and phasing in of secure and interoperable technologies.

Congress should work with accreditation organizations like The Joint Commission and with government agencies to produce an incentive program, perhaps through Medicare and Medicaid reimbursements, to phase out legacy systems. Stronger privacy and security requirements for replacement systems can further help bolster system cybersecurity.

Recommendation #4.2: Learn from the financial sector's success in sector-specific cybersecurity investment, spearheaded by the National Cybersecurity Center of Excellence (NCCoE).

In the financial sector, large players with requisite capital have acquired cybersecurity companies so as to have them tailor their products to the industry's specific needs. NIST's NCCoE should not fund or develop the technologies, but it can serve as a coordinating body to bring together major healthcare players with the capacity to emulate the financial sector model—based on a three-tier framework of universal platform technologies, industry-specific technologies, and subsector-specific technologies.

Recommendation #4.3: Leverage a broad array of existing funding programs to spur healthcare cybersecurity basic research and innovation.

The government should spearhead the creation of a program to inform where healthcare cybersecurity may be going in the next five years, and future research strategies that could inform that thinking. This should include a net assessment of existing research and development efforts in this arena, and a focus on concentrating R&D around insider threat detection, IoT medical device security, and AI technologies for privacy and security.

Recommendation #4.4: Create mechanisms for clarifying privacy standards, providing advice, and receiving feedback from health systems.

The OCR at HHS should convene experts and stakeholders to develop better guidance and definitions around HIPAA privacy and security compliance. This can be coupled with existing punitive measures to encourage fewer violations.

Recommendation #4.5: Strengthen FDA requirements around medical device security, to ensure that security is baked-in at every point in the device's life cycle.

The FDA should add a requirement for end-to-end secure system development lifecycle (SDLC) for medical devices, to ensure more robust security by design. This should be coupled with transitional support such as trainings, public outreach, and site visits to help steer device manufacturers towards better cybersecurity practices.

Workforce

Recommendation #5.1: Amend the Cybersecurity Enhancement Act of 2014 to incentivize recipients of the CyberCorps Scholarship to serve in specific, critical need sectors like healthcare.

Congress should allow CyberCorps Scholarship recipients to pursue work outside of strictly government organizations, which would open up far more opportunities in healthcare. The *Cyber Scholarship Opportunities Act* (S. 754) introduced in the Senate in 2017 may help accomplish this goal.

Recommendation #5.2: The US Department of Labor, HHS, and state and local governments should enable models for cybersecurity apprenticeships in the healthcare sector.

NCCoE should coordinate the development of a framework for healthcare cybersecurity apprenticeship programs in particular (going beyond just information technology). Federal and state policymakers should then take action to incentivize the creation of such programs, including through subsidies provided to employers, tax breaks, or public service agreements similar to the CyberCorps Scholarship.

Recommendation #5.3: Create and incentivize adoption of sector-specific Centers of Academic Excellence (CAE) designated programs.

DHS and the NSA should work with stakeholders to develop specific CAE designations for higher education institutions focused on critical infrastructure sectors like healthcare. In addition to the competitive and/or brand advantage this may provide a higher education institution, Congress can incentivize pursuit of such CAE certifications by backing it with potential research funding.

Recommendation #5.4: Support an industry-wide approach for creating a healthcare cybersecurity certification.

NIST should convene stakeholders to inform the creation of a healthcare cybersecurity certification, including industry associations, training providers, professional organizations, hiring managers, and healthcare industry leadership. This certification should focus on healthcare-specific cybersecurity issues, cover the spectrum of junior and senior healthcare employees, and recognize the need for jobs doable by workers with less than five years of professional experience.

Recommendation #5.5: Create a sustainable financing model that supports healthcare providers who typically have the least concentration of cybersecurity expertise.

The federal government should develop programs to increase healthcare professional retention and rural and small- and medium-sized organizations, such as through direct grants or loan repayment programs.

Recommendation #5.6: Provide payroll tax incentives to healthcare providers to address the "brain drain" in healthcare cybersecurity.

Federal and state policymakers should offer tax incentives for organizations retaining the same cybersecurity professional in a position for a minimum number of years. Through this baseline and other possible additions like an increased benefit for each amount of time beyond the minimum, governments can encourage healthcare organizations to better staff their cybersecurity needs.

Recommendation #5.7: Empower employees with artificial intelligence and automation tools for time- and data-intensive tasks in order to maximize productivity and reduce burnout.

To maximize productivity and reduce burnout, healthcare organizations should adapt their institutional policies to focus on technologies that can automate time-intensive tasks and allow for efficient review of large patient data sets. This can enable organizations to focus their resources on other priorities like investigating incidents.

Notes

1 *Robert Lord, John Cmar, "HIV patients forced to choose between medical care and their privacy," Becker's Hospital Review, July 24, 2018.*

2 *Beyond an individual's personal electronic health record, EHRs are also critical to understanding medical devices, software, and other healthcare infrastructures because they are largely interconnected by an underlying system of EHRs.*

3 *Health Care Industry Cybersecurity Task Force, Report on Improving Cybersecurity in the Healthcare Industry, June 2017.*

4 *Dr. Dale Needham's Outcomes After Critical Illness and Surgery (OACIS) Research Group*

5 *Pronovost, P., Needham, D., Berenholtz, S., Sinopoli, D., Chu, H., Cosgrove, S., . . . Goeschel, C. (2006). An intervention to decrease catheter-related bloodstream infections in the ICU. The New England Journal of Medicine, 355(26), 2725– 2732.*

6 *Challen R, Denny J, Pitt M, et alArtificial intelligence, bias and clinical safetyBMJ Quality & Safety 2019;28:231-237, https://qualitysafety.bmj.com/content/28/3/231*

7 *For example see: The UK Comptroller & Auditer General, 'Investigation: WannaCry cyber attack and the NHS', UK National Audit Office, April 25, 2018, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf*

8 *Robert H. Shmerling, "First, Do No Harm," Harvard Health Publishing, October 13, 2015.*

9 *US Food and Drug Administration, Content of Premarket Submission for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration (Washington DC, FDA, Oct 2018) Staffhttps://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf*

10 *US Department of Health and Human Services, Public Health Emergency: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (Washington DC, HHS, Dec 2018) https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx*

11 *Healthcare and Public Health Sector Coordinating Council, Medical Device and Health IT Joint Security Plan (Healthcare and Public Health Sector Coordinating Council, Jan 2019) https://healthsectorcouncil.org/the-joint-security-plan/*

12 *National Institute of Standards and Technology, Cybersecurity Framework Version 1.1 (Gaithersburg MD, NIST, April 2018) https://www.nist.gov/cyberframework/framework*

13 *Andrew Simmonds, Peter Sandilands, Louis van Ekert, "An Ontology for Network Security Attacks", Applied Computing, 2004.*

14 *Penelope Hughes JD MPH, Vaishali Patel PhD MPH, Joy Pritts JD. "Health care providers' role in protecting EHRs: Implications for consumer support of EHRs, HIE and patient-provider communication." ONC Data Brief, no 15 (Washington, DC: Office of the National Coordinator for Health Information Technology. February 2014). https://www.healthit.gov/sites/default/files/022414_hit_attitudesaboutprivacydatabrief.pdf*

15 *McAfee, McAfee Labs Threats Report March 2018 (March, 2018) https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2018.pdf*

16 *McAfee, McAfee Labs Threats Report September 2018 (September, 2018) https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf*

17 *U.S. Food & Drug Administration, St. Jude Medical Recalls Implantable Cardioverter Defibrillators (ICD) and Cardiac Resynchronization Therapy Defibrillators (CRT-D) Due to Premature Battery Depletion, February 16, 2018; Jim Finkle, "J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking," Reuters, October 4, 2016.*

18 *S.G. Shini, Tony Thomas, and K. Chithraranjan, "Cloud Based Medical Image Exchange-Security Challenges," Procedia Engineering 38 (2012): 3454-3461; HIPAA Journal, Touchstone Medical Imaging Suffers 307K Patient Data Breach, October 21, 2014, https://www.hipaajournal.com/touchstone-medical-imaging-suffers-307k-patient-data-breach/*

19 *Ryan Francis, "Healthcare Records for Sale on Dark Web," CSO Online, April 24, 2017.*

20 *For a U.S. definition of critical infrastructure sectors, see https://www.dhs.gov/cisa/critical-infrastructure-sectors*

21 *We acknowledge this philosophy is idealized, especially as many of the contributors have worked in a clinical context, but we prefer to hope for the best possible world, while planning for the reality that we have.*

22 *U.S. Federal Register, "Request for Information on Modifying HIPAA Rules To Improve Coordinated Care," December 14, 2018. https://www.federalregister.gov/documents/2018/12/14/2018-27162/request-for-information-on-modifying-hipaa-rules-to-improve-coordinated-care*

23 *Fred Donovan, "OCR Drafts NPRM on 'Good Faith' Patient Data Disclosure Rules," HealthIT Security, October 19, 2018. https://healthitsecurity.com/news/ocr-drafts-nprm-on-good-faith-patient-data-disclosure-rules*

24 *One prominent example of this was the March 2016 MedStar ransomware attack that compromised a well-known vulnerability and led to immediate and complete loss of health system information, according to MedStar's director of emergency management during the attack, Craig DeAtley. For more, see Dr. John L. Hick, "Lessons Learned from the MedStar Health System Outage: An Interview with Craig DeAtley, PA-C," The Exchange Volume 1 Issue 2, 2016.*

25 *One prominent example of this was the 2015 Anthem, Inc. attack, in which nearly 80 million member and employee records—including such personal information as name, home address, Social Security number, and birth date—were stolen by a cyber espionage group. See coverage of the Anthem, Inc. Affiliated Covered Entity incident first submitted to HHS OCR on March 13, 2015: Bob Herman, "Details of Anthem's Massive Cyberattack Remain in the Dark a Year Later," Modern Healthcare, March 30, 2016.*

26 *Michelle Andrews , The Rise of Medical Identity Theft, Consumer Reports online (Consumer Reports, August 25, 2016) https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/*

27 *Health Care Industry Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry (Washington, D.C.: Department of Health and Human Services, 2017). (Hereafter: Cybersecurity Task Force, Report).*

28 *Verizon, Verizon 2018 Data Breach Investigations Report, 5, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf. (Hereafter: Verizon, 2018 DBIR).*

29 *According to the Indiana University Knowledge Database, phishing attacks "are typically fraudulent email messages appearing to come from legitimate enterprises (e.g., your university, your internet service provider, your bank). These messages usually direct you to a spoofed website or otherwise get you to divulge private information (e.g., passphrase, credit card, or other account updates)" that can then be used to commit a crime or gain unlawful entry to your wider network. See: Indiana University, Avoid Phishing Scams, July 16, 2018, https://kb.iu.edu/d/arsf*

30 *United Kingdom National Audit Office, Investigati on: WannaCry cyber attack and the NHS (London, United Kingdom: U.K. Department of Health, 2017); CBS News, "Global Cyberattack Strikes Dozens of Countries, Cripples U.K. Hospitals," CBS News, May 12, 2017. (Hereafter: CBS "Global Cyberattacks").*

31 *Josh Beckerman, "Newkirk Products Reports Data Breach," The Wall Street Journal, August 5, 2016; Jessica Davis, "OCR Investigating Banner Health for 2016 Breach of 3.7 Million Patient Records," Healthcar e IT News, March 21, 2018.*

32 *Brian Fung, "Computer Security Experts Fear Second Wave of 'Biggest Ransomware Attack Ever,'" T he Washington Post, May 14, 2017. (Hereafter: Fung, "Experts Fear Ransomware Attack").*

33 *Fred Donovan, "Cass Regional Finally Recovers from Devastating Ransomware Attack," HealthIT Security, July 18, 2018.*

34 *U.S. Department of Health & Human Services, Su bmitting Notice of a Breach to the Secretary, January 5, 2015, https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html*

35 *"Notification to the Secretary," Code of Federal Regulations, title 45 (2011): https://www.gpo.gov/fdsys/granule/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-408*

36 *Protenus, Inc. and DataBreaches.net, Breach Barometer 2017 Report, 8-14. (Hereafter: Protenus, Bre ach Barometer).*

37 *Susan Morrow, "Top 10 Threats to Healthcare Security," Infosec Institute, January 8, 2018.*

38 *These attacks wirelessly block, typically through encryption, a clinic's access to patient health records and/or connected medical devices, disrupting the delivery of patient care and demanding payment to return access to compromised systems. Global attacks of this nature occured in 2017 when a vulnerability in an outdated version of the Microsoft Windows operating system was exploited in various legacy medical devices, thus disrupting patient care and causing permanent loss of health data and IT systems. For more, see: Tim Johnson, "How the Dark Overlord is costing U.S. clinics big time with ransom demands," Providence Journal, May 29, 2017; CBS "Global Cyberattacks"; Fung, "Experts Fear Ransomware Attack"; Alex Hern, "NHS Could Have Avoided WannaCry Hack with 'Basic IT Security', Says Report," The Guardian, October 26, 2017.*

39 *Verizon, 2018 DBIR, 34.*

40 *Joe Uchill, "Health-care Group Pushes for Tighter Email Security Amid Fears Over Fraud," The Hill, November 28, 2017.*

41 *Healthcare Information and Management Systems Society, 2018 HIMSS Cybersecurity Survey (Chicago, IL: Healthcare Information and Management Systems Society, 2018).*

42 *Verizon, 2018 DBIR, 33.*

43 *DataBreaches.net, Fairbanks Hospital Notifies Patients After Discovering Employees Could Have Been Inappropriately Accessing Patient Records for Years (UPDATED), December 22, 2016. (Hereafter: Fairbanks Discovery).*

44 *Protenus, Breach Barometer, 2017.*

45 *The Darkweb is a portion of the global internet intentionally hidden from public access behind passwords and other controls.*

46 *Richard, "The Value of Stolen Data on the Dark Web," Dark Web News, July 1, 2017.*

47 *Ibid.*

48 *Michael Kan, "Here's How Much Your Identity Goes for on the Dark Web," PCMag, November 15, 2017.*

49 *Charles Ornstein, "Small-Scale Violations of Medical Privacy Often Cause the Most Harm," ProPublica, December 10, 2015.*

50 *Charles Ornstein, "Celebrities' Medical Records Tempt Hospital Workers to Snoop," National Public Radio, December 10, 2015.*

51 *Anna Gorman and Abby Sewell, "Six People Fired from Cedars-Sinai Over Patient Privacy Breaches," Lo s Angeles Times, July 12, 2013; Stephanie Innes, "3 UMC Workers Fired for Record Access," Arizona Daily Star, January 12, 2011.*

52 *Michael Kranish, "IRS is Overwhelmed by Identity Theft Fraud," Boston Globe, February 16, 2014.*

53 *Ponemon Institute, Cost of a Data Breach Study: Global Overview (Traverse City, MI: Ponemon Institute, 2018). (Hereafter: Ponemon, Breach Study).*

54 *The number of physicians and hospitals using at least a basic EHR in 2008 was only 17 percent and nine percent, respectively. By 2015, however, the number of hospitals and physicians using even more robust certified EHR technologies had skyrocketed to 96 percent and 78 percent, respectively. For more, see: The Office of the National Coordinator for Health Information Technology, 2016 Report to Congress on Health IT Progress: Examining the HITECH Act and the Future of Health IT (Washington, DC: Department of Health and Human Services, 2016).*

55 *The number of connected things in use worldwide, including medical devices, wearables, and mobile phones, was more than 8 billion in 2017 and will reach 20.4 billion by 2020. The market for global connected medical devices is expected to reach "$1.34 billion by 2021 at a growth rate of 26 percent." For more, see: Bill Kleyman, "The Future of Edge Healthcare Services and HIT Infrastructure," HIT Infrastructure, February 26, 2018; Elizabeth O'Dowd, "Health IT Connected Medical Device Market on the Rise," HIT Infrastructure, October 24, 2016.*

56 *Dimiter Dimitrov, "Medical Internet of Things and Big Data in Healthcare," Healthcare Informatics Research 22 (July 2016): 156-163.*

57 *Min Chen, Yixue Hao, Kai Hwang, Lu Wang, Lin Wang, "Disease Prediction by Machine Learning Over Big Data From Healthcare Communities," IEEE Access Volume 5 (April 26, 2017): 8869-8879.*

58 *Yichuan Wang, LeeAnn Kung, Terry Anthony Byrd, "Big Data Analytics: Understanding its capabilities and potential benefits for healthcare organizations," S cienceDirect Volume 126 (January 2018): 3-13.*

59 *Andrew Burt and Samuel Volchenboum, "How Health Care Changes When Algorithms Start Making Diagnoses," Harvard Business Review, May 08, 2018.*

60 *We would also like to note a counterargument posed by some very thoughtful commentators on this topic - notably that before HITECH, there were no standards for cybersecurity, and there was a very bad state of healthcare cybersecurity investment even before the 2009 incentives, minimizing the extent to which you can lay our current predicament at the feet of these incentives. We concur—we think that a fair characterization of healthcare cybersecurity is that it was bad before HITECH, it was on balance made worse by the explosion in EHRs, but that there were certainly some good security and privacy innovations that came from regulators through Meaningful Use requirements and other federal incentives.*

61 *Linda T. Kohn, Janet M. Corrigan, Molla S. Donaldson, To Err Is Human, The National Academies of Sciences Engineering Medicine, November 1999.*

62 *Alex B. Haynes, Thomas G. Weiser, William R. Berry, et al 'A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population' The New England Journal of Medicine 360: 491, Jan 29, 2009 https://www.nejm.org/doi/full/10.1056/NEJMsa0810119*

63 *Protenus, Breach Barometer.*

64 *Statistics drawn from the American Hospital Association's 2016 AHA Annual Survey, which is the most recent version of the survey to be released at time of publication: AHA, Fast Facts 2018.*

65 *For instance, hybrid clouds. A hybrid cloud infrastructure combines on-site infrastructure with external, third-party provided cloud services and requires the on-site provider (hospital, physician, etc.) to secure their own infrastructures. This hybrid structure introduces new end-to-end compliance and data security issues: TLP White, "FDA MD Plan, NIST Updates, Hybrid Could ICANN," NH-ISAC National Healthcare, April 24, 2018; Bill Siwicki, "A Supercomputer Center Shows the Security Challenges of Operating a Healthcare Hybrid Cloud," Healthcare IT News, April 18, 2018.*

66 *Thomas Fox-Brewster, "Watching The Awful WannaCry Ransomware Scourge Hit Doctor's Surgeries IRL," Forbes, May 15, 2017; Swati Khandelwal, "FDA Recalls Nearly Half a Million Pacemakers Over Hacking Fears," Hacker News, August 21, 2017.*

67 *U.S. House of Representatives Committee on Oversight and Reform, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," September 7, 2016. https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/*

68 *Ben Davis, "GDPR requires privacy by design, but what is it and how can marketers comply?" Econsultancy, August 25, 2017. https://econsultancy.com/gdpr-requires-privacy-by-design-but-what-is-it-and-how-can-marketers-comply/*

69 *GDPR, Article 25*

70 *Margins in not-for-profit and public health systems also dropped from an average of 3.5 percent in FY 2015 to just 2.7 percent in FY 2016. For some comparison, estimated margins in the real estate development and brokerage and investment banking sectors are at 13.45 and 15.01 percent, respectively. Kelly Gooch, "Moody's: US nonprofit hospitals see decrease in median operation margin," Becker's Healthcare, May 17, 2017 in reference to Moody's, Prel iminary FY 2016 US NFP Hospital Medians Edge Lower on Revenue, Expense Pressure, May 16 2017. (Hereafter: Moody's, Preliminary FY 2016); NYU Stern, Operating Net Margins, 2018.*

71 *New York University Stern School of Business, Ope rating Net Margins by Sector (US), January 2018. (Hereafter: NYU Stern, Operating Net Margins, 2018).*

72 *Cybersecurity Task Force, Report, 35.*

73 *Elizabeth Snell, "Why Healthcare Cybersecurity Budgets Should Increase," HealthITSecurity, July 31, 2017.*

74 *Ge Bai, John Xuefeng Jiang, Renee Flasher, Hospi tal Risk of Data Breaches, JAMA Network, April 3, 2017.*

75 *NIST, "NIST Cybersecurity Framework", 2018. https://www.nist.gov/cyberframework*

76 *ISO, "ISO/IEC 27000:2018", https://www.iso.org/standard/73906.html*

77 *Thanks to Dr. David Mussington for pointing this out.*

78 *This is according to an Axios report that found healthcare margins in large-sized healthcare organizations can be up to 6.7 percent on average when accounting for Wall Street investments, mergers, and other investment options; however, this margin is still below the 7.9 percent cross-sector average. Full report here: Chris Canipe and Andrew Witherspoon, Not-for-profit Hospital Systems: 2016-17 Financials, Axios. https://www.axios.com/hospitals-are-making-a-fortune-on-wall-street-1513388345-1b7e1923-e778-4627-8fcc-bfab39e2d5c4.html (Herafter: Not-for-Profit Hospital Systems, 2016-2017).*

79 *Not-for-Profit Hospital Systems, 2016-2017.*

80 *In a statement, the American Hospital Association (AHA) cited the high cost of prescription drugs, increased regulatory burdens, and funding shortfalls in Medicaid and Medicare as leading reasons for the difficulty in keeping pace. According to AHA, regulatory burdens alone cost their constituents $39 billion a year. See the AHA report here: Regulatory Overload Report, American Hospital Association, October 2017.*

81 *Jessica Davis, "West Virginia Hospital Replaces Computers After Petya Cyberattack", Healthcare IT News, June 30, 2017. https://www.healthcareitnews.com/news/west-virginia-hospital-replaces-computers-after-petya-cyberattack*

82 *Ponemon, Medical Device Security.*

83 *Thanks again to Dr. David Mussington for helping frame this problem.*

84 *Emily Lawson and Colin Price, "The Psychology of Change Management," McKinsey Quarterly, June 2003. (Hereafter: Lawson and Price, 2003.)*

85 *This recommendation originated from the 2017 OCR-NIST conference.*

86 *U.S. Department of Health and Human Services, "Compliance & Enforcement: Resolution Agreements and Civil Money Penalties," https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html*

87 *Lawson and Price, 2003.*

88 *U.S. Department of Health and Human Services, "Compliance & Enforcement: Case Examples," https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/index.html*

89 *FDA, Expedited Access Pathway Program, February 8, 2018.*

90 *For additional information on this, see the May 24, 2018 letter from the AMA to the Committee on Energy and Commerce.*

91 *In 2004, California became the first state to enact legislation that required hospitals to meet a minimum registered nurse to patient ratio. The intent of the law was to improve patient outcomes and "although no consensus has yet been reached, studies have shown that the law has improved patient care in a variety of domains."(See: J. Paul Leigh, "California's Nurse-to-Patient Ratio Law Reduced Nurse Injuries by More Than 30 Percent," Economic Policy Institute, March 3, 2015). In addition, the same research found that the number of nurse injuries also dropped after implementation of the safe nurse to patient ratio. This program evolved from a critical need to protect patients, nurses, and healthcare providers. The law works by mandating that for every X patients, there must be at least Y nurses to treat them, ensuring a minimum ratio of nurses to patients and appropriate "coverage" based on the complexity of care being provided. While simple, it is elegant in its message: one cannot achieve excessive efficiencies at the cost of good patient care.*

92 *These examples come from the UCISA Information Security Management Toolkit. https://www.ucisa.ac.uk/ismt*

93 *Examples of this sort of preliminary work include research from Ge Bai, John Jiang, Renee Flasher, Hos pitals Risks of Data Breaches, JAMA Internal Medicine, 2017, 177(6), 878-880.*

94 *21st Century Oncology Holdings, the global cancer care company mentioned in Recommendation #3.1, filed for bankruptcy around two years after its breach of 2.2 million patient records. The breach was only one of many disreputable behaviors that brought its downfall, but the $2.3 million fine from the HHS certainly did not help. https://www.news-press.com/story/news/2018/01/09/21st-century-oncology-announces-bankruptcy-plan-approval/1017786001/*

95 *Thank you to Michael Daniel for providing this insight.*

96 *The Cybersecurity Disclosure Act requires publicly traded companies to disclose to the SEC the level of cybersecurity expertise at the board level or, if no such expertise exists, report on other cybersecurity steps that were taken into account by the company (see: Senate Committee on Banking, Housing, and Urban Affairs, Cybersecurity Disclosure Act of 2017, 115th Cong., 1st. Sess., 2017, S. 536.).*

97 *New York's cyber regulation requires financial institutions to comply with a number of cybersecurity measures: "to have a cybersecurity program designed to protect consumers' private data; a written policy or policies that are approved by the board or a senior officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial services industry." (see: New York State, DFS Cybersecurity Regulation Compliance Requirements Are Effective Today, August 28, 2017, htt ps://www.dfs.ny.gov/about/press/pr1708281.htm.)*

98 *For these examples and others, see the February 26, 2018 letter from the AMA to the Office of Inspector General. https://searchlf.ama-assn.org/undefined/documentDownload?uri=/unstructured/binary/letter/LETTERS/2018-5-24-Letter-to-Walden-Pallone-re-Draft-Cybersecurity-Response-to-EC-RFI.pdf*

99 *Ibid.*

100 *American Hospital Association, "Legal (Fraud and Abuse) Barriers To Care Transformation and How to Address Them," February 28, 2017. https://www.aha.org/system/files/content/16/barrierstocare-full.pdf*

101 *Russell Branzell (College of Healthcare Information Management Executives (CHIME) CEO) & Cletis Earle (Chair, CHIME Board of Trustees), Letter to Daniel R. Levinson, Inspector General for the US Department of Health and Human Services dated Oct 26, 2018 (CHIME website, Oct 2018) https://chimecentral.org/wp-content/uploads/2018/10/CHIME-letter-to-OIG-on-AKS-FINAL-V2.pdf*

102 *Greg Garcia, Executive Director for Cybersecurity, Healthcare Sector Coordinating Council, Letter to Susan Edwards, Associate Counsel, Office of the Inspector General for the US Department of Health and Human Services dated October 26, 2018 (Healthcare Sector Coordinating Council website, Oct 2018) https://healthsectorcouncil.org/wp-content/uploads/2018/10/HSCC-CWG-Comments-on-HHS-OIG-Anti-Kickback-Statute-RFI.pdf*

103 *The CMS had an open request for information regarding the regulatory burdens of the Stark Law for two months, ending on August 24, 2018. For more see: Centers for Medicare & Medicaid Services, "Medicare Program; Request for Information Regarding the Physician Self-Referral Law," Federal Register (Washington, D.C.: June 25, 2018). https://www.federalregister.gov/documents/2018/06/25/2018-13529/medicare-program-request-for-information-regarding-the-physician-self-referral-law*

104 *See the CMS's December 27, 2013 revisions. Centers for Medicare & Medicaid Services, "Medicare Program; Physicians' Referrals to Health Care Entities With Which They Have Financial Relationships: Exception for Certain Electronic Health Records Arrangements," Federal Register (Washington, D.C.: December 27, 2013) https://www.federalregister.gov/documents/2013/12/27/2013-30923/medicare-program-physicians-referrals-to-health-care-entities-with-which-they-have-financial*

105 *Protenus, Breach Barometer; Verizon, 2018 DBIR; Ponemon, Breach Study.*

106 *This idea was floated as a "Cash for Clunkers" style program in the Cybersecurity Task Force, Report , 29. We would like to credit the idea of phasing out legacy technologies to the Task Force, but also provide an alternative pathway to achieving a meaningful transition. We also recommend using*

different language to describe this program since "Cash for Clunkers" was created during a specific political context that may be negatively perceived by some constituencies.

107 *I Am the Cavalry, Hippocratic Oath for Connected Medical Devices, January 19, 2016.*

108 *Cybersecurity Task Force, Report, 1.*

109 *Ibid., 28.*

110 *The WannaCry ransomware attacks exploited vulnerabilities on devices running outdated or unpatched versions of an old Windows operating system, encrypting the system and demanding that the users of infected systems pay a ransom to regain control of their devices. Because a large number of medical devices ran this legacy version of Windows, a large number of these devices were affected, shutting down health systems around the world. According to a post-incident investigation conducted by England's National Health Service (NHS), thousands of appointments were cancelled and medical care had to be triaged just to maintain emergency care services. Even still, five acute trusts, or hospital trusts that provide secondary care in the United Kingdom—including in London—were forced to divert emergency patients to other departments. Without the fortuitous intervention of a cybersecurity researcher who stumbled upon a "kill switch" that effectively stopped the spread of the bug, even more disruption would have occurred. Yet, according to the NHS report, "all organisations infected by WannaCry shared the same vulnerability and could have taken relatively simple action to protect themselves," such as updating or patching known software flaws in their legacy devices that had been previously flagged by the national healthcare IT partner, NHS Digital.*

111 *According to the Verizon 2015 DBIR, 99.9 percent of "exploited vulnerabilities had been compromised more than a year after the associated CVE [Common Vulnerabilities and Exposures report] was published." Verizon, Verizon 2015 Data Breach Investigations Report (New York, NY: Verizon, Inc., 2015). (Hereafter: Verizon, 2015 DBIR).*

112 *Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend (Tra verse City, MI: Ponemon Institute, 2017). (Hereafter: Ponemon, Medical Device Security).*

113 *Ibid.*

114 *Ibid.*

115 *Symantec, Addressing Healthcare Cybersecurity Strategically (Mountain View, CA: Symantec Corporation); David B. Black, "Security Regulations vs. Cyber-security: The War," Huffington Post, May 2, 2017; Amit Kulkarni, "Why HIPAA Compliance Does Not Equal Data Security," Health IT Outcomes, August 9, 2016.*

116 *U.S. Department of Homeland Security, Healthcare and Public Health Sector-Specific Plan, p. 9, May 2016.*

117 *Thanks to Matt Doan for this insight.*

118 *Cybersecurity Task Force, Report.*

119 *Office of the Inspector General U.S. Department of Health & Human Services, A Roadmap for New Physicians: Fraud & Abuse Laws, July 17, 2018.*

120 *This observation and an initial set of recommendations was first brought to our attention by the excellent work of the June 2017 Health Care Cyber Security Task Force Report, which we will continue to build upon. See Cybersecurity Task Force, Report, 27.*

121 *For example, static and dynamic application analysis, code review, and penetration testing.*

122 *Ponemon, Medical Device Security.*

123 *U.S. Food and Drug Administration, Quality System (QS) Regulation/Medical Device Good Manufacturing Practices, March 27, 2018. https://*

www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/QualitySystemsRegulations/default.htm. (Hereafter: FDA Medical Device Regulation)

124 *More specifically, the FDA's cybersecurity guidance for premarket medical device development can be found in: U.S. Food and Drug Administration, C ontent of Premarket Submissions for Management of Cybersecurity in Medical Devices (Silver Spring, MD: Food and Drug Administration, 2014); and U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices: Guidance for Food and Drug Administration Staff (Silver Spring, MD: Food and Drug Administration, 2016) (henceforth: U.S. Food and Drug Administration, "Postmarket Management.").*

125 *Elizabeth Snell, "How FDA Medical Device Cybersecurity Guidance Affects Providers," HealthIT Security. https://healthitsecurity.com/features/how-fda-medical-device-cybersecurity-guidance-affects-providers*

126 *U.S. Food and Drug Administration, "Postmarket Management," 13.*

127 *Ibid.*

128 *Cybersecurity experts will readily note that lack of testing is but one of many factors contributing to the proliferation of vulnerabilities. This example is given to show that regulations lag far behind even some of the most basic cybersecurity practices.*

129 *For more, see Cybersecurity Task Force, Report, 30-31.*

130 *Cybersecurity Task Force, Report, 28-29. The Report focuses primarily on actions that industry can take to phase out legacy technology, and also correctly calls for government action to "consider incentives, requirements, and/or guidelines for reporting and/or use of unsupported [legacy] system[s]." The Report also calls for "incentive recommendations to phase-out legacy and insecure health care technologies." Our report goes one step further in providing an even more specific plan for how to achieve this phasing-out.*

131 *Thanks to Josh Corman and Beau Woods from I Am The Cavalry for their tremendous help with these recommendations.*

132 *U.S. Congress, House, Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S.1691, 115th Cong., 1st sess., introduced in Senate August 1, 2017. h ttps://www.congress.gov/bill/115th-congress/senate-bill/1691/actions*

133 *Ali Breland, "White House Unveils Report on Modernizing IT," The Hill, December 13, 2017. http://thehill.com/policy/technology/364724-white-house-release-federal-it-guidance*

134 *See, generally, Chapter 1 of this report in the section on "Vulnerabilities and Consequences."*

135 *For examples of such incubators, see: Neil Ainger, Barclays sign eight FinTech start-ups and spinoff 'intrapreneur' CNBC.com (CNBC website, May 4 2017, updated May 5 2017) https://www.cnbc.com/2017/05/04/barclays-sign-eight-fintech-start-ups-and-spinoff-intrapreneur.html and JP Morgan Chase In Residence, (JPMC website, accessed Aug 25 2019) https://www.jpmorgan.com/global/in-residence*

136 *For example of such an incubator, see: Tamaya Macheel, Goldman Sachs launches in-house incubator, Tearsheet, March 15, 2018 https://www.tearsheet.co/funding/goldman-sachs-launches-in-house-incubator*

137 *Jon Oltsik, "What is a Cybersecurity Technology Platform Anyway?" CSO Online, April 27 2018, https://www.csoonline.com/article/3269398/security/what-is-a-cybersecurity-technology-platform-anyway.html*

138 *National Cybersecurity Center of Excellence, Securing Electronic Health Records on Mobile Devices*

(Gaithersburg, MD: National Institute of Standards and Technology, 2015); National Cybersecurity Center of Excellence, Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector (Gaithersburg, MD: National Institute of Standards and Technology, 2017); National Cybersecurity Center of Excellence, Securing Wireless Infusion Pumps In Healthcare Delivery Organizations (Gaithersburg, MD: National Institute of Standards and Technology, 2017).

139 *Some useful information on existing research efforts can be found on the U.S. National Library of Medicine website (https://www.nlm.nih.gov/hsrinfo/electronic_health_record.html#872Grants).*

140 *Charles W. Wessner, "Recommendations and Findings," in The Small Business Innovation Research Program (SBIR): An Assessment of the Department of Defense Fast Track Initiative (Washington, DC: National Academy Press, 2000), 32.*

141 *Ibid., "Preface", 5.*

142 *Ibid., "Introduction", 27.*

143 *Ibid., "Recommendations and Findings," 33.*

144 *Ibid., 35.*

145 *For a more detailed explanation on how to calculate social rates of return, see the study by Link and Scott "Estimates of the Social Returns to Small Business Innovation Research Projects," in Ibid., 275.*

146 *The Department of Defense, through its "Defense Advanced Research Projects Agency" (DARPA), began funding SEMATECH in 1987. See more: DARPA, SEMATECH, July 17, 2018 https://www.darpa.mil/about-us/timeline/sematech*

147 *NIST, NIST Advanced Technology Program Launches 54 New Technology R&D Projects, October 4, 2000.*

148 *National Research Council, Review of the Research program of the Partnership for a New Generation of Vehicles: Fourth Report (Washington, DC: The National Academies Press, 1998).*

149 *In the interest of full disclosure, please note that this specific area, also known as "Healthcare Compliance Analytics" is the core business of Robert Lord, one of the co-authors of this paper*

150 *These were the preliminary results from Phase 2 of the HIPAA Audit Program. Full report available at: Linda Sanches, "Update on Audits of Entity Compliance with the HIPAA Rules" (Washington DC, Office for Civil Rights (OCR), U.S. Department of Health and Human Services, September, 2017) https://www.nist.gov/sites/default/files/documents////sanches_0.pdf*

151 *See the AMIA's response to the ONC's RFI concerning EHR reporting. Douglas B. Fridsma, President and CEO of the American Medical Informatics Association, Letter to The Honorable Donald Rucker, MD, National Coordinator for Health Information Technology, US Department of Health and Human Services ('Re: Request for Information Regarding the 21st Century Cures Act Electronic Health Record Reporting Program') dated October 17, 2018 (AMIA website, October 2018) https://www.regulations.gov/document?D=HHS-ONC-2018-0022-0072*

152 *FDA Medical Device Regulation.*

153 *FDA, " Content of Premarket Submissions for Management of Cybersecurity in Medical Devices", October 18, 2018. www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529*

154 *Thanks to David Holtzman for helping articulate this point.*

155 *It is worth mentioning from the outset that many terms (including workforce gap, workforce shortage, skills shortage, talent shortfall, etc.) may be used*

more or less interchangeably throughout this chapter. While each phrase has some specific contextual nuance, they all help describe some aspect of the same problem. This problem is specifically related to the gap caused by an increasing demand for cybersecurity employees and the inability or inefficiency of hiring managers to fill those positions.

156 *Frost & Sullivan, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk (San Antonio, TX: Frost & Sullivan, 2017). (Hereafter: Frost & Sullivan, Workforce Study).*

157 *Ibid.*

158 *Laura Bate, Alternative Pathways to Cybersecurity Education, (Washington, DC: New America, 2018). (Hereafter: Bate, Alternative Pathways).*

159 *Bate, Alternative Pathways.*

160 *Katherine W. Phillips, "How Diversity Makes Us Smarter," Scientific American, October 1, 2014. (Hereafter: Phillips, "Diversity"); ISC2, (ISC)² Study Finds U.S. Minority Cybersecurity Professionals Underrepresented in Senior Roles, March 15, 2018. (Hereafter: ISC2, Minority Study).*

161 *NYU Stern, Operating Net Margins, 2018; Moody's, Preliminary FY 2016.*

162 *ISC2, Hiring and Retaining Top Cybersecurity Talent: What Employers Need to Know About Cybersecurity Jobseekers in 2018, (Clearwater, FL: ISC2, 2018).*

163 *Michael Minear, a CIO for a California health system, described this problem in a recent Modern Healthcare report. After investing time and money to train a talented staff of cybersecurity specialists, two of Minear's original five team members were poached by other companies. It took Minear a year and a half to fill those job openings. This example perfectly illustrates the vexing problem facing healthcare managers: as it grows increasingly difficult to fill open positions, it becomes equally difficult to hold on to top talent. This is an all-too-common challenge for healthcare managers. See the full report at: Joseph Conn, "Healthcare Struggles to Recruit Top Cybersecurity Pros," Modern Healthcare, October 14, 2015. (Hereafter: Healthcare Struggles to Recruit Top Cybersecurity Pros).*

164 *See "Healthcare Struggles to Recruit Top Cybersecurity Pros."*

165 *Bronwyn Mauldin, Apprenticeships in the Healthcare Industry (Washington, DC: Department of Labor, 2011).*

166 *Burning Glass Technologies and General Assembly, Blurring Lines: How Business and Technology Skills Are Merging to Create High Opportunity Hybrid Jobs (Boston, MA: Burning Glass Technologies, 2018).*

167 *Cybersecurity experts will readily note that existing applications can already identify these types of anomalies. However, many healthcare organizations (especially small- and medium-sized organizations) do not currently use these applications.*

168 *Andrea Limbago, Increasing Retention Capacity: Research from the Field (Arlington, VA: Endgame, 2017). (Hereafter: Limbago, Retention Capacity).*

169 *Frost & Sullivan, Workforce Study*

170 *Ibid.*

171 *ISC2, Minority Study.*

172 *Frost & Sullivan, 2017 Global Information Security Workforce Study: Women in Cybersecurity (San Antonio, TX: Frost & Sullivan, 2017). Anecdotal evidence from our external reviewers suggests that female participation rates in cybersecurity in healthcare are higher than other communities, but more empirical data is needed to state this claim conclusively.*

173 *Phillips, "Diversity".*

174 *National Science Foundation, CyberCorps: Scholarship for Service Recognizes First Hall of Fame Recipients, January 10, 2018.*

175 *AHA, Fast Facts 2018.*

176 *See a committee mark-up version of Senate Bill 754, which passed the Commerce Committee unanimously: U.S. Congress, House, Cyber Scholarship Opportunities Act of 2017, S.754, 115th Cong., 1st sess., introduced in Senate March 28, 2017.*

177 *Critical national infrastructures are here defined according to the Critical Infrastructures Protection Act of 2001: "The term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." See: Critical Infrastructures Protection Act, 42 U.S. Code § 5195c (2001).*

178 *Apprenticeship is defined by the DOL as "an arrangement that includes a paid-work component and an educational or instructional component, wherein an individual obtains workplace-relevant knowledge and skills." Well-established and registered apprenticeship models exist in many industries including construction, hospitality, transportation, and advanced manufacturing." See: Exec. Order. No. 13801, 82 Fed. Reg. 28229 (June 15, 2017), https://www.whitehouse.gov/presidential-actions/3245/*

179 *Virtual Career Network, Apprenticeship Training Healthcare, July 17, 2018.*

180 *Importantly, the recognition of an occupation as "apprenticeable" does not necessarily lead to the creation of an actual apprenticeship program, as that responsibility rests primarily with state and local jurisdictions and private apprenticeship organizations. The Department of Labor's Career One Stop apprenticeship database has listed an "Information Assurance Specialist" position at the Spectrum Health-Butterworth Campus in Michigan, but it appears to still be in development. It is difficult to identify any other single existing healthcare cybersecurity apprenticeship. See: Career OneStop, A pprenticeship Finder, July 17, 2018.*

181
Mary Alice McCarthy, Iris Palmer, Michael Prebil, Con necting Apprenticeship and Higher Education: Eight Recommendations (Washington, DC: New America, 2017).

182 *According to Brent Parton in the Youth Apprenticeship in America Today report from New America (Washington, DC: New America, 2017), behind every successful youth apprenticeship program in the U.S., "there is an intermediary holding the partnership (between apprentices and employers) together." Simply put, intermediaries are individuals and organizations that coordinate the activity of key partners, including employers and apprentices, to ensure a program's success. Importantly, not all intermediaries are firms that require payment for their services. In fact, many of the most successful intermediaries are individuals who do this work for free. While many intermediaries are private, for-profit organizations, they are often under-resourced and (in the case of individuals completing this work) typically do not coordinate apprenticeships as a full-time aspect of their job.*

183 *For more on the strategies to scale apprenticeship capacity, see: Ibid.; Mary Alice McCarthy, Iris Palmer, and Michael Prebil, Connectin g Apprenticeship and Higher Education: Eight Recommendations (Washington, DC: New America, 2017).*

184 *Employment and Training Administration, Using Registered Apprenticeship to Build and Fill Healthcare Career Paths (Washington, DC: Department of Labor, 2011). (Hereafter: Using Registered Apprenticeships in Healthcare).*

185 *Ibid.*

186 *For instance, the first cybersecurity apprenticeship program in Virginia, which is generally viewed as a leader in this space, didn't begin accepting students until 2017.*

187 *A good example is the Good Samaritan Society's partnership with the University of South Dakota. This program allows apprentices working towards a Certified Nursing Assistant designation to complete their curriculum requirements via distance learning, so they can take online classes in whatever location they are currently based. See: Using Registered Apprenticeships in Healthcare.*

188 *Aurore Le Bris and Walid El Asri, State of Cybersecurity & Cyber Threats in Healthcare Organizations: Applied Cybersecurity Strategy for Managers (Cergy-Pontoise, France: Essec Business School, 2017).*

189 *While healthcare organizations should ideally distinguish IT from cybersecurity, this does not always happen.*

190 *The goal of this initiative is to identify and designate certain higher education and research institutions according to their commitments to robust cybersecurity degree programs and cybersecurity-related knowledge units. These CAE institutions can be 2-year community and technical colleges, 4-year bachelor's degree granting universities, specialized training centers, or military schools. Along with the formal recognition from the US government that brings prestige and publicity, students attending CAE designated institutions can apply for certain scholarships and grants; however, there is no guarantee that funding will be provided to all of the centers that earn the CAE designation. For more on the CAE program, see: National Initiative for Cybersecurity Careers and Studies, National Centers of Academic Excellence (CAE), July 17, 2018.*

191 *National Science Foundation, Secure and Trustworthy Cyberspace (SaTC), July 17, 2018. For even more information on cybersecurity and STEM education-specific NSF grants, see the STELAR Webinar from June 14, 2018: http://stelar.edc.org/events/stelar-webinar-nsf-opportunities-broadening-participation-stem-1*

192 *Cybersecurity certifications used to demonstrate a cybersecurity professional's capabilities already exist in abundance. The sheer number of certifications creates a veritable alphabet soup of qualifications that can be confusing for experts and newcomers, alike. Some of the more popular cybersecurity certifications include the Certified Information Systems Security Privacy Professional (CISSP), Certified Information Systems Auditor (CISA), CompTIA Security+, and the Global Information Assurance Certification (GIAC). There is even a CompTIA Healthcare IT Certification focused on integrating essential healthcare and IT terminologies (this certification is NOT focused on information security; only one unit, the shortest unit of the entire certification process, is dedicated to security). Each credential can be useful to signal an individual's skills and competencies in using specific tools or platforms, making certifications highly desirable for hiring managers. In fact, a third of all cybersecurity jobs call for some kind of industry certification. For more on cybersecurity certifications, see: Burning Glass, Job Market Intelligence: Cybersecurity Jobs, 2015, (Boston, MA: Burning Glass Technologies, 2015). For more on the CompTIA Healthcare IT Certification, see: National Initiative for Cybersecurity Careers and Studies, CompTIA® Healthcare IT Certification Training, July 17, 2018.*

193 *CompTIA, CompTIA Security+ Certification, July 17, 2018, https://certification.comptia.org/certifications/security*

194 *GIAC, Certifications: Pricing, July 17, 2018, https://www.giac.org/certifications/pricing*

195 *ISC2, Certified Information Systems Security Professional, July 17, 2018, https://www.isc2.org/Certifications/CISSP*

196 *Certifications like the "Associate of (ISC)2" can provide alternative certifications for individuals who lack the sufficient work experience for other certifications, like CISSP; however, it is not clear whether employers consider this a useful certification and, of course, it is a moot point when job postings typically require years of work experience in addition to certifications.*

197 *Typically, companies set these sorts of standards on their own. But there may be some opportunity to include a broader range of stakeholders relevant to the creation of a healthcare cybersecurity certification (e.g. academia, industry, and government), perhaps through a group like the NICE Training and Certifications Sub Working Group: https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/training-and-certifications-sub-working-group*

198 *Burning Glass, The Narrow Ladder: The Value of Industry Certifications in the Job Market (Boston, MA: Burning Glass Technologies, 2017).*

199 *Cybersecurity Task Force, Report.*

200 *Frost & Sullivan, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk (San Antonio, TX: Frost & Sullivan, 2017).*

201 *For one example of this, See: Fairbank Discovery; The 2017 Breach Barometer Report: Mid-Year Review from Protenus, Inc. in collaboration with Databreaches.net also provides a good summary: Protenus, Breach Barometer.*

202 *Andrew Chamberlain and Morgan Smart, Why Do Workers Quit? The Factors That Predict Employee Turnover (Mill Valley, CA: Glassdoor, Inc., 2017).*

203 *Derek Thompson, "Health Care Just Became the U.S.'s Largest Employer" (The Atlantic, January 9, 2018)*

NEW AMERICA