HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

Members of the Task Force

The following 21 individuals constitute the membership of the Health Care Industry Cybersecurity Task Force established in March 2016.

- **Task Force Co-Chair Emery Csulak, MS, CISSP, PMP,** Chief Information Security Officer, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services

- **Task Force Co-Chair Theresa Meadows, MS, RN, CHCIO, FHIMSS, FACHE,** Senior Vice President and Chief Information Officer, Cook Children's Health Care System

- **Joshua Corman,** Co-Founder, I Am The Cavalry

- **George DeCesare, JD,** Senior Vice President and Chief Technology Risk Officer, Kaiser Permanente

- **Anura Fernando,** Principal Engineer, Medical Software and Systems Interoperability Health Sciences Division, UL LLC

- **David Finn, CISA, CISM, CRISC,** Health Information Technology Officer, Symantec Corp.

- **Mark Jarrett, MD, MBA, MS,** Senior Vice President and Chief Quality Officer, Northwell Health and Professor of Medicine, Hofstra Northwell School of Medicine

- **Laura Laybourn,** Senior Advisor, Office of Cyber and Infrastructure Analysis, National Protection and Programs Directorate, U.S. Department of Homeland Security

- **Michael McNeil,** Global Product Security and Service Officer, Philips Healthcare

- **Dan McWhorter,** Vice President and Chief Intelligence Strategist, FireEye, Inc.

- **Roy Mellinger, CISSP-ISSAP, ISSMP, CIM,** Vice President, IT Security and Chief Information Security Officer, Anthem, Inc.

- **Jacki Monson, JD, CHC, CHPC,** Vice President, Chief Privacy and Information Security Officer, Sutter Health

- **Ram Ramadoss, MBA, CISA, CISM, CISSP, CRISC, CIPP,** Vice President, CRP Privacy and Information Security and EHR Compliance Oversight, Catholic Health Initiatives

- **Terry Rice,** Vice President, IT Risk Management and Chief Information Security Officer, Merck & Co.

- **Vito Sardanopoli, CISM, CISSP, CISA,** Senior Director of Enterprise Security Services and Governance, Quest Diagnostics

- **Rob Suarez,** Director of Corporate Product Security, BD

- **Kevin Stine,** Chief, Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology

- **Christine Sublett, MA, CISSP, CIPT, CRISC, CGEIT,** Chief Information Security Officer and Head of Compliance, Augmedix, Inc.

- **Lauren Thompson, PhD,** Director, Interagency Program Office, Defense Health Management Systems, Department of Defense / Department of Veterans Affairs

- **David Ting,** Co-Founder and Chief Technology Officer, Imprivata, Inc.

- **Fred Trotter,** Data Journalist, CareSet Systems

The members of the Health Care Industry Cybersecurity Task Force would like to thank all of the individuals and organizations that contributed the development of this report. Contributors include: Stephen Curren, Aftin Ross PhD, MAJ (U.S. Army) William B. Marsh RN, Thad Odderstol, Alissa Johnson PhD., Jason Cameron, Donna Dodson, Ben Flatgard, Kathryn Martin, Nickol Todd, Rose-Marie Nsahlai, Stephen Niemczak, Lucia Savage, Adam Sedgewick, Malikah Smith, Richard Struse, Scott Vantrease, Mark Weber, Nicole Edison, Margie Zuk, Penny Chase, Darren Leitsch, Joanna Centola, Kenneth Trumpoldt, Ryan Marinella, and Christopher Hernandez.

The Task Force would also like to express its gratitude to the Department of Health and Human Services, the Department of Homeland Security, and the National Institute of Standards and Technology for their work to establish and support the Task Force throughout its efforts.

June 2, 2017

The Honorable Lamar Alexander
Chairman
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
United States House of Representatives

The Honorable Ron Johnson
Chairman
U.S. Senate Committee on Homeland Security and Government Affairs

The Honorable Michael McCaul
Chairman
Homeland Security Committee
United States House of Representatives

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate

The Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
United States House of Representatives

Dear Chairman Alexander, Chairman Burr, Chairman Johnson, Chairman McCaul, Chairman Nunes, and Chairman Walden:

On behalf of the Health Care Industry Cybersecurity Task Force, we are pleased to submit to you this Report on Improving Health Care Industry Cybersecurity.

The *Cybersecurity Act of 2015* provided a much needed opportunity to convene public and private sector subject matter experts to spend the last year discussing and developing recommendations on the growing challenge of cyber attacks targeting health care. Twenty-one Task Force members contributed to this effort, including 17 from private sector organizations. As public and private sector Co-Chairs of the Task Force, we worked diligently to balance industry and government perspectives and to solicit input from outside stakeholders and the general public.

The Task Force's discussions resulted in the development of six imperatives along with cascading recommendations and action items. All of these reflect the need for a unified effort – among public and private sector organizations of all sizes and across all sub-sectors – to work together to meet an urgent challenge. They also reflect a shared understanding that for the health care industry cybersecurity issues are, at their heart, patient safety issues. As health care becomes increasingly dependent on information technology, our ability to protect our systems will have an ever greater impact on the health of the patients we serve. While much of what we recommend will require hard work, difficult decisions, and commitment of resources, we will be encouraged and unified by our shared values as health care industry professionals and our commitment to providing safe, high quality care.

We invite you to join us as we continue to advance this very important mission. We thank you for your support of the Task Force and look forward to the opportunity to brief you on our findings.

Sincerely,

/s/ Emery Csulak

Emery Csulak
Co-Chair
Chief Information Security Officer and
Senior Official for Privacy
Centers for Medicare and Medicaid Services

/s/ Theresa Meadows

Theresa Meadows
Co-Chair
Senior Vice President and Chief Information Officer
Cook Children's Health Care System

Contents

Figures and Tables

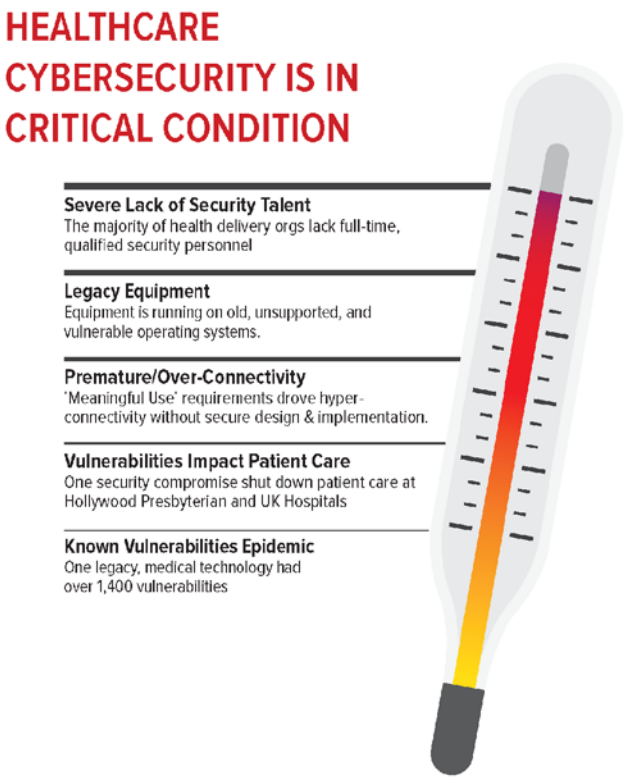
This page intentionally left blank.

Executive Summary

The health care system cannot deliver effective and safe care without deeper digital connectivity. If the health care system is connected, but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs. Our nation must find a way to prevent our patients from being forced to choose between connectivity and security.

In the *Cybersecurity Act of 2015* (the Act), Congress established the Health Care Industry Cybersecurity (HCIC) Task Force to address the challenges the health care industry faces when securing and protecting itself against cybersecurity incidents, whether intentional or unintentional. Real cases of identity theft, ransomware, and targeted nation-state hacking prove that our health care data is vulnerable. Data collected for the good of patients and used to develop new treatments can be used for nefarious purposes such as fraud, identity theft, supply chain disruptions, the theft of research and development, and stock manipulation. Most importantly, cybersecurity attacks disrupt patient care (References to Figure 1 found below)[1].

Figure 1 Health Care Cybersecurity Environment



The health care industry in the United States is a mosaic, including very large health systems, single physician practices, public and private payers, research institutions, medical device developers and software companies, and a diverse and widespread patient population. Layered on top of this is a matrix of well-intentioned federal and state laws and regulations that can impede addressing issues across jurisdictions. This creates the potential to develop barriers to innovation and ease of use. Within this complex network, patients must be protected from harms that may stem from cybersecurity vulnerabilities and exploits.

Now more than ever, all health care delivery organizations (including all constituents referred to above) have a greater responsibility to secure their systems, medical devices, and patient data. Most health care organizations face significant resource constraints as operating margins can be below one percent. Many organizations cannot afford to retain in-house information security

[1]2013 HIMSS Security Survey - pg 34: Severe Lack of Security Talent; Naked Security, "Windows XP Still Widespread Among Healthcare Providers": Legacy Equipment; HealthIT.gov, "Meaningful Use Definition & Objective": Premature / Over-Connectivity; ArsTechnica, "Patients diverted to other hospitals after ransomware locks down key software": Vulnerabilities cause Patient Care Outages; ICS-CERT, "Advisory (ICSMA-16-089-01) CareFusion Pyxis SupplyStation System Vulnerabilities": Known vulnerabilities epidemic

personnel, or designate an information technology (IT) staff member with cybersecurity as a collateral duty. These organizations often lack the infrastructure to identify and track threats, the capacity to analyze and translate the threat data they receive into actionable information, and the capability to act on that information. Many organizations also have not crossed the digital divide in not having the technology resources and expertise to address current and emerging cybersecurity threats. These organizations may not know that they have experienced an attack until long after it has occurred. Additionally, both large and small health care delivery organizations struggle with numerous unsupported legacy systems that cannot easily be replaced (hardware, software and operating systems) with large numbers of vulnerabilities and few modern countermeasures. Industry will need to dramatically reduce the use of less defensible legacy and unsupported products, and more effectively reduce risk in future products through robust development and support strategies.

With the exception of IT security personnel, many providers and other health care workers often assume that the IT network and the devices they support function efficiently and that their level of cybersecurity vulnerability is low. Recent high-profile incidents, such as ransomware attacks and large-scale privacy breaches, have shown this vulnerability assumption to be false and provided an opportunity to increase education and awareness about the benefits of cybersecurity in the health care community. Moreover, recent ransomware incidents have also highlighted how patient care at health care delivery organizations can be interrupted due to a system compromise. Members of the health ecosystem reported that prior to these breaches many security professionals had difficulty demonstrating the importance of cyber protections to organizational leadership, including how risk mitigation can save money and protect against reputational damage in the long-term. Making the decision to prioritize cybersecurity within the health care industry requires culture shifts and increased communication to and from leadership, as well as changes in the way providers perform their duties in the clinical environment.

Thus, health care cybersecurity is a key public health concern that needs immediate and aggressive attention. In consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, the Secretary of Health and Human Services brought together a diverse group of industry representatives to discuss these issues, consistent with the requirements outlined in the Act. Industry participation in the Task Force brought to light critical areas for discussion. Some of the topics raised included:

- Who from the federal government provides cybersecurity leadership and coordinates the preparedness and response for cybersecurity incidents for the health care sector? (Recommendation 1.1)

- How does industry organize itself to oversee and promote health care cybersecurity priorities and share information? (Recommendation 1.4, Recommendation 4.5, Recommendation 6.2)

- How does the sector leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or other frameworks, as a standard to measure itself, as well as to design and implement risk management practices? (Recommendation 1.2)

- What impact does the diversity of regulations have on the ease of adoption of cybersecurity practices or the ability of industry members to collaborate on cybersecurity issues? (Recommendation 1.3, Recommendation 1.5)

- How do legacy systems (including medical devices, electronic health records, etc.) affect health care industry cybersecurity and how can these systems be made more resilient? (Recommendation 2.1)

- What are the cybersecurity challenges facing small and rural organizations? (Recommendation 3.3, Recommendation 3.4, Recommendation 6.1)

- How does supply chain affect the secure development, on-going maintenance, and system hardening (i.e., managing vulnerabilities in third party software) for medical devices, pharmaceutical manufacturing, and Internet of Things innovation? (Recommendation 2.2, Recommendation 2.3)

To identify a wide range of threats that affect the health care industry, the Task Force relied on information gathered during public meetings, briefings and consultations with experts on a variety of topics across health care and other critical infrastructure sectors, internal Task Force meetings, and responses to blog posts.[2] The Task Force's activities resulted in the development of recommendations that will collectively help increase security across the health care industry. The Task Force identified six high-level imperatives by which to organize its recommendations and action items. The imperatives are:

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.

2. Increase the security and resilience of medical devices and health IT.

3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.

4. Increase health care industry readiness through improved cybersecurity awareness and education.

5. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.

6. Improve information sharing of industry threats, weaknesses, and mitigations.

[2] The Act identifies members of the health care industry to include: health plans, health care clearinghouses, or health care providers; patient advocates; pharmacists; developers of health information technology; laboratories; pharmaceutical or medical device manufacturers; and other additional stakeholders in the definition of health care industry stakeholders.

Each recommendation includes one or more action items for implementing the recommendation. Some recommendations and action items identify a single entity that the Task Force recommends be responsible for the recommendation and action items, while other recommendations and action items recommend multiple entities be responsible for implementation. The successful implementation of these recommendations will require adequate resources and coordination across the public and private sector. Once implemented, the recommendations will increase security for the health care industry's organizations, networks, and associated medical devices. See Appendix A for a summary of the imperatives, recommendations, and action items contained in this report.

The public-private partnership cultivated by the Task Force, which resulted in the development of this report, has provided an opportunity to address significant cybersecurity concerns in the health care industry. The Task Force members found this engagement with other federal and private sector partners beneficial to understand our common cybersecurity challenges and concerns. Therefore, we believe the establishment of an ongoing public-private forum would serve to enhance cybersecurity discussions and protections as a critical component for the health care industry to increase patient safety.

I. Health Care Industry Cybersecurity Task Force Charge and Approach

Cybersecurity concerns are bi-partisan and figure prominently into the platforms of both the Republican and Democratic parties. This was demonstrated when Congress passed the *Cybersecurity Act of 2015* (the Act). Given the severity of attacks in recent years and the rapid deployment of information technology (IT) throughout health care, Congress singled out the health care industry and required the establishment of the Health Care Industry Cybersecurity Task Force (HCIC Task Force or Task Force). Under Section 405 (c), the Act required the Task Force to accomplish six tasks that culminated in the development and delivery of the Task Force's *Report on Improving Cybersecurity in the Health Care Industry*. Just as the 1999 Institute of Medicine report *To Err is Human*[3] was a call to arms for patient safety, the Task Force hopes that this report galvanizes both the public and private sectors to comprehensively address cybersecurity challenges in order to protect patients. Under the Act, the Task Force was directed to:

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for implementing title I of this division, so that the Federal Government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

To accomplish its mandate the Department of Health and Human Services (HHS), Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST) identified Task Force members representing the federal government, hospitals, insurers, patient advocates, security researchers, pharmaceutical companies, medical device manufacturers, health IT developers and vendors, and laboratories. Collectively, the members possess both depth and breadth of expertise in IT and cybersecurity, clinical medicine, medical device development, and

[3] Institute of Medicine. (1999). *To Err is Human: Building a Safer Health System*. Retrieved from: Building a Safer Health System Report

software development. The Task Force's approach to meeting the Act Section 405 (c) requirements included holding internal meetings at least monthly, engaging the public through four public meetings, consulting with experts within health care and other critical infrastructure sectors, and gathering additional insight and information from the public through responses to blog posts. Appendix B summarizes all meetings held by the Task Force.

The Task Force received briefings and consultations from experts from other critical infrastructure sectors on a variety of topics to understand their strategies and safeguards for addressing cybersecurity threats. Specifically, the Task Force engaged members of the Financial Services, Transportation, and Energy Sectors. Despite some similarities between these sectors and health care, the Task Force realized that if every health care organization were required to immediately implement the highest level of cybersecurity best practices, many would be forced to choose between – as one Task Force member stated – procuring new security technologies and related subject matter expertise, or purchasing new ventilators and hiring nurses. See Appendix D for documented cybersecurity best practices from other critical infrastructure sectors.

Health care data may be used for a variety of nefarious purposes including fraud, identity theft, supply chain disruptions, the theft and sale of proprietary information, stock manipulation, and disruption of hospital systems and patient care. A significant challenge and vulnerability for providers, hospitals, pharmaceutical manufacturers, and laboratories includes the ever-increasing volume of connected medical devices and automated medication delivery systems, which, if not protected, could pose a risk to patient safety. Industry participation on the Task Force identified critical areas for discussion. Some of the topics raised included:

- Who from the federal government provides cybersecurity leadership and coordinates the preparedness and response for cybersecurity incidents for the health care sector? (Recommendation 1.1)

- How does industry organize itself to oversee and promote health care cybersecurity priorities and share information? (Recommendation 1.4, Recommendation 4.5, Recommendation 6.2)

- How does the sector leverage the NIST Cybersecurity Framework, or other frameworks, as a standard to measure itself, as well as to design and implement risk management practices? (Recommendation 1.2)

- What impact does the diversity of regulations have on the ease of adoption of cybersecurity practices or the ability of industry members to collaborate on cybersecurity issues? (Recommendation 1.3, Recommendation 1.5)

- How do legacy systems (including medical devices, electronic health records, etc.) affect health care industry cybersecurity and how can these systems be made more resilient? (Recommendation 2.1)

- What are the cybersecurity challenges facing small and rural organizations? (Recommendation 3.3, Recommendation 3.4, Recommendation 6.1)

- How does supply chain effect the secure development, on-going maintenance, and system hardening (i.e., managing vulnerabilities in third party software) for medical devices, pharmaceutical manufacturing, and Internet of Things (IoT) innovation? (Recommendation 2.2, Recommendation 2.3)

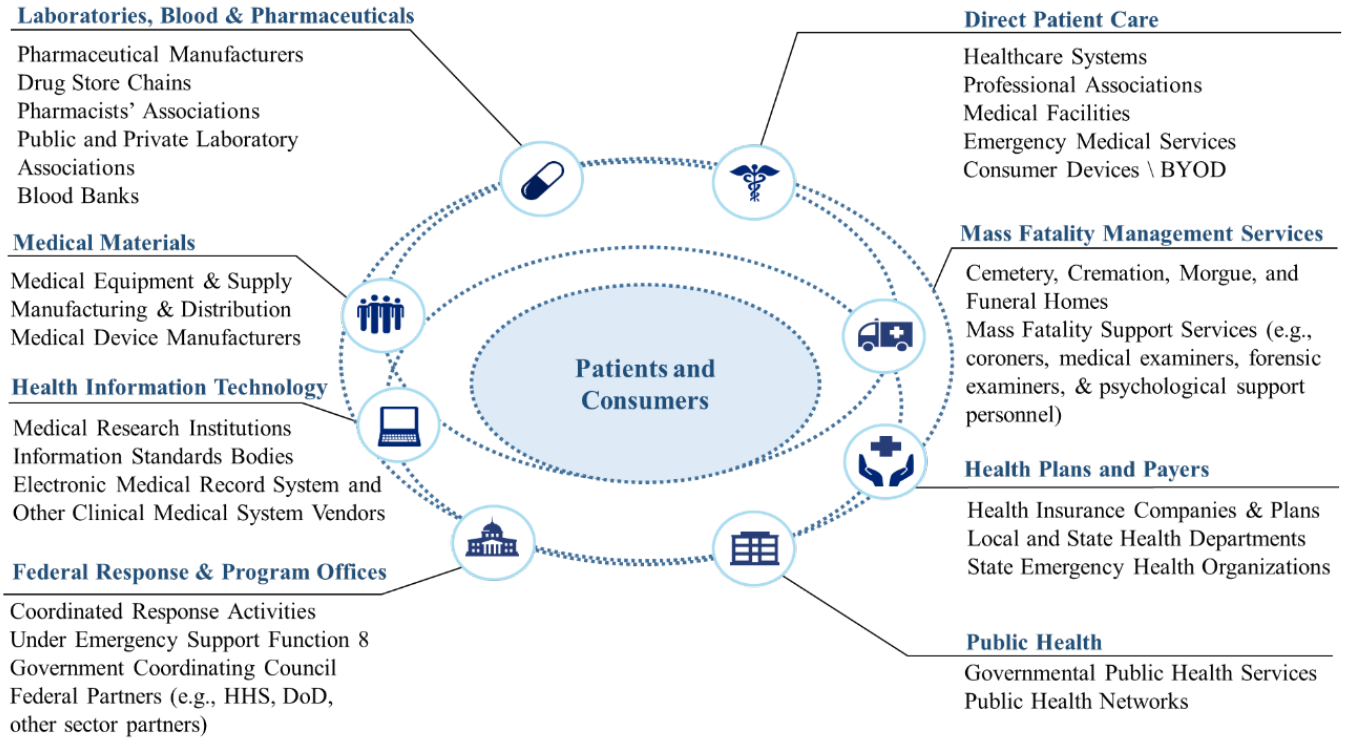
The Task Force discussions highlighted the benefits of engaging in focused conversations between stakeholders across the health care industry; the Task Force encourages the continued coordination and cooperation between industry and the federal government.

II. The State of Cybersecurity within the Health Care Industry

Organization of the Health Care Industry

The Health Care and Public Health (HPH)[4] Sector Coordinating Council and Government Coordinating Council define health care in their 2016 Sector Specific Plan as "large, diverse, and open… It includes publicly accessible health care facilities, research centers, suppliers, manufacturers, and other physical assets. It also includes vast, complex public-private information technology systems required for care delivery and for supporting the rapid, secure transmission and storage of large amounts of health care data."[5] The HPH Sector represents approximately nine percent of the total United States (U.S.) workforce.[6] See Figure 2 for a depiction of the sector as documented in the HPH Sector Specific Plan and as discussed by the HCIC Task Force.

Figure 2 Health Care Ecosystem



[4] This report references both the health care industry and HPH Sector. Instances of "HPH Sector" refers to all subsectors as defined in the HPH Sector Specific Plan, and instances of "health care industry" refers to the health care subsectors addressed in this report. *Healthcare and Public Health Sector-Specific Plan*. (2016). Retrieved from: DSH HPH Sector Plan

[5] *Healthcare and Public Health Sector-Specific Plan*. (2016). Retrieved from: DHS HPH Sector Plan

[6] The Henry J. Kaiser Family Foundation. (2015). *Healthcare Employment as a Percentage of Total Employment*. Retrieved from: Statistics of healthcare employment

Unique Culture

Health care has an open, sharing culture—as is appropriate to support its primary mission—but this culture also complicates the issues of security and privacy. Providers spend a majority of their financial and personnel resources to help as many patients as possible. The number of patients, families, and providers involved daily in the process of health care is enormous. The need to access information quickly to provide patient care needs has to be balanced with the need for cybersecurity protections. To respond to critical care issues quickly and maintain a seamless workflow, health care personnel may leave workstations unlocked and unattended to expedite access to patient information and to share data with clinicians in order to provide comprehensive care. While leaving workstations unlocked improves the speed with which a provider can access the patient's information and identify potentially lifesaving allergies or drug interactions, these practices could lead to the loss, unauthorized access, or alteration of patient data. Additionally, hospitals are also 'public' institutions that are open 24 hours a day, seven days a week, and 365 days per year. They are open to everyone who is looking for medical care and to visitors who may be known to patients but not to staff. Hospital staffing is also constantly changing, and often utilizes rotating or temporary staff, including physicians. Many hospitals also utilize volunteers who are not always as trained or as skilled as staff.

Within the health care industry, cybersecurity has historically been viewed as an IT challenge, is approached reactively, and is often not seen as a solution that can help protect the patient. Additionally, limited financial resources, the use of legacy devices that were not designed to resist or even recognize the cyber attacks of today, a lack of understanding of the risks cyber threats pose, and limited education and awareness programs for health care professionals increases the impacts that cyber threats could have on the sector. Members of the health care industry report that without experiencing a breach or data loss, many security professionals and organizations have difficulty demonstrating the importance of cyber protections and how proactive risk mitigation can save money and protect against reputational damage in the long-term. Making the decision to prioritize and resource cybersecurity in health care will require organizational culture shifts and increased support and direction from leadership, as well as changes to the way providers perform their duties in clinical environments.

Digital Transformation

The evolution of IT in other critical infrastructure sectors occurred over the course of decades. This allowed organizations to organically determine what processes would benefit from automation and for their awareness of cybersecurity threats to evolve along with their technical infrastructure. For a variety of reasons, such as protecting patient privacy, the health care industry was slow to embrace data digitization. Years of avoiding automation contributed to rising health care costs which have become a steadily growing percentage of our national gross domestic product.[7] This lagging adoption prompted the federal government to

> Over the next few years, most machinery and technology involved in patient care will connect to the Internet; however, a majority of this equipment was not originally intended to be Internet accessible, nor designed to resist cyber attacks.

[7] The World Bank. (2016). *Health expenditure, total (% of GDP)*. Retrieved from: Information retrieved from The World Bank

subsidize the adoption of EHRs. This incentive increased EHR adoption from approximately 9.4 percent to 96 percent of non-federal acute care hospitals.[8]

In the recent past, any health care or patient data leaving a system or provider space had to be printed, read, and transcribed prior to being ingested at a receiving facility. This paper-based system helped to protect the health care industry from cyber threats and the exposure of patient information, but greatly slowed the collaborative nature of a connected and interoperable care system. Initial digital record keeping was limited to the data required to demonstrate that medical billing occurred correctly. This digital information was protected by simply keeping all digital data in-house and behind the firewall.

In the last decade, the health care industry evolved past the limited capabilities of digital billing records and adopted EHRs as a standard tool for documentation and workflow. With this adoption and widespread use of EHRs, effort was originally placed on installing hardware and software required to earn the incentives. Unfortunately, a majority of the health care sector made financial investments in cybersecurity only in the last five years.[9] At the same time, the health care industry connected digital systems to the Internet and began to realize both the benefits and consequences that can result from that level of interconnectivity. In some cases, the mere connection between two devices such as a glucose monitor and an insulin delivery system can provide profound benefits to both health care professionals and patients. However, this connectivity increases clinical dependence on technologies that support life maintaining and lifesaving operations. If these technologies are not protected, the integrity or availability of an IV pump or a radiation medicine device could be impacted and this has the potential to harm patients.[10]

Patients and physicians have derived many benefits from EHRs including giving patients the ability to access their information through portals and giving providers the ability to more easily share patient information. However, this digitization resulted in an increased attack surface for health care providers, medical device companies, and many other parts of the health care industry. In some cases, interoperability efforts increased patient safety risks due to the introduction of unsecure solutions, such as a patient portal accessible over the public Internet with limited security controls in place, or the rapid development of EHRs with minimal standardization or guiding security best practices. The Centers for Medicare & Medicaid Services (CMS) was willing to pay providers to have a patient portal. Since 2005, the *Health Insurance Portability and Accountability Act* (HIPAA) Security Rule required providers to implement safeguards to ensure the confidentiality, integrity, and

> "The EHR represents the ability to easily share medical information among stakeholders and to have a patient's information follow him or her through the various modalities of care engaged by that individual." EHRs are designed to be accessed by all people involved in the patients care—including the patients themselves."
>
> ~ Health IT Buzz

[8] Advisory Board (2016) *ONC: EHR adoption rates on the rise, but barriers to interoperability remain.* Retrieved from Advisory Board Daily Briefing

[9] Institute for Critical Infrastructure Technology. (2016). *Hacking Healthcare IT in 2016*. Retrieved from: ICIT Brief regarding Hacking Healthcare IT in 2016

[10] ABC 7 News. (2017). *San Mateo cyber security firm uncovers malware on medical devices*. Retrieved from: ABC 7 News report regarding San Mateo cyber security firm

availability of protected health information (PHI); however, many providers lacked the expertise and/or resources to implement security and privacy measures to properly secure these portals.

The volume of connected medical devices and automated medication delivery systems has increased. Most medical devices were not originally designed to directly communicate with users such as health care providers, biomedical engineers, patients, consumers, or other devices. Nevertheless, medical device users expect to see that data today. Therefore, securing health care data and medical devices, consumer and clinical, is essential to protecting patients and providing them with the highest level of care.

This challenge is expected to increase as health care becomes more dependent upon the IoT, including non-regulated devices that may affect privacy, safety, and patient care. These may include such diverse products as manufacturing systems, building control systems, and wearable devices. In addition, precision medicine[11] (which customizes treatment based on a patient's environment, lifestyle, and genes) is likely to provide great benefits to patient care while also generating potential risks as information is shared.

Some health care organizations across the sector, including providers, manufacturers, and large payers, have successfully managed the digital transformation and are on par with the Financial Services Sector in implementing cyber protections. However, less mature entities have yet to understand or implement these protections due to a lack of awareness, financial resources, or staff. Given the level of interconnectivity and diversity within the sector, the interdependency of subsectors on one another, and the disparity between organizations' ability to address cybersecurity issues, health care as a whole will only be as secure as the weakest link.

If providers and patients are to develop and sustain trust in the digital component of the health care system that is necessary for inoperability, the health care industry must prioritize cybersecurity thinking across the continuum of health care. Such thinking can help shift cybersecurity from solely a security and IT priority to a much broader cultural change and organizational issue that is designed to keep patients safe from digitally-sourced harm.

Regulatory Environment

The response of the federal government to improving critical infrastructure cybersecurity in the health care sector is multi-pronged. Within the HHS, the Office for Civil Rights (OCR), CMS, the Food and Drug Administration (FDA), the Office of the National Coordinator (ONC), and the Office of the Assistant Secretary for Preparedness and Response (ASPR) play important and diverse roles in cybersecurity. Other administrative agencies and independent commissions, for example, the Federal Trade Commission (FTC) also play a role in setting expectations for privacy and security of health information.

The multiplicity of actors in this space is often necessary to address a wide range of cybersecurity challenges and system types, and can be helpful in allowing these challenges to be viewed and addressed from multiple perspectives. It also has the potential to create complications. Some entities may be subject to regulation and oversight by multiple federal government entities, each with their own rules, which may be difficult to reconcile. Product and technology innovations for medical devices and health IT outpace the development and creation

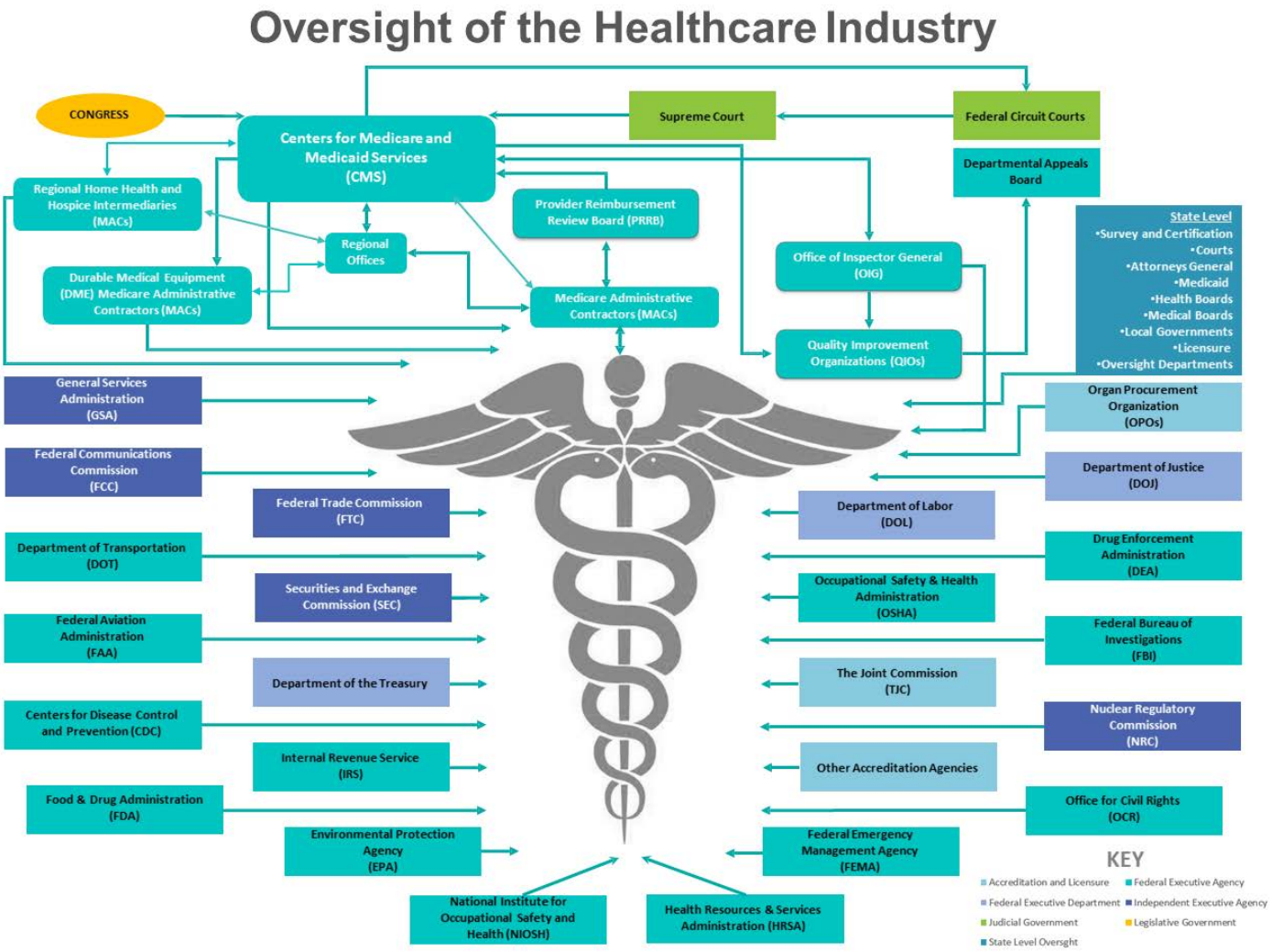
[11] According to the National Institutes of Health, "Precision medicine is an emerging approach for disease treatment and prevention that takes into account individual variability in environment, lifestyle and genes for each person." NIH. (2016). *About the All of Us Research Program*. Retrieved from: NIH Precision Medicine

of regulations. While many regulations that apply to cybersecurity in health care are well-meaning and individually effective, taken together they can impose a substantial legal and technical burden on health care organizations. These organizations must continually review and interpret multiple regulations, some of which are vague, redundant, or both. In addition, organizations must dedicate resources to implement policy directives that may not have a material impact on reducing risks.

At the same time, gaps in protections can leave key health care unaddressed and create holes in cybersecurity infrastructure for health information. Consider, for example, the different roles of FDA and OCR with respect to health information cybersecurity. FDA is charged with ensuring approved and cleared medical devices are safe and efficacious, whereas OCR is charged with oversight of the privacy and security regulations under HIPAA, which applies only to "covered entities" (e.g., most health care providers, health plans, and health care clearinghouses), and contractors acting on their behalf, known as "business associates." With the recent publication of the FDA's final guidance for manufacturers on device cybersecurity, the FDA has taken more steps to address the patient safety concerns generated by cybersecurity risks to medical devices. However, FDA oversight is limited to patient safety and does not extend to patient privacy. HIPAA's regulations focus on both privacy and security; however, medical device manufacturers may not be covered entities or business associates under HIPAA. This leaves a health care provider using a medical device with potentially greater responsibility for assuring privacy and security protections for health information created and shared by the device. While many stakeholders agree that protecting against cybersecurity threats should be a shared responsibility, to date, health care providers have shouldered an inordinate amount of the burden even when actions needed to improve security in the device have been outside their control.

The challenges around the push and pull of the regulatory complexity associated with ensuring patient safety and patient privacy is growing with an increasing amount of information that is being shared digitally and the proliferation of the use of devices. The *Health Information Technology for Economic and Clinical Health Act* spurred investment in EHRs through billions of dollars of incentives to hospitals and clinicians under the "Meaningful Use" of EHR program. The Meaningful Use program combined with the Merit-Based Incentive Payment System will continue to push providers to use EHRs and other technologies to exchange patient information electronically. In addition, alternate payment models of care which rely heavily on the use of health IT combined with the increased capacity of medical devices to store a growing amount of PHI, means more patient data is at risk for cybersecurity attacks. Data collected for the good of the patients and used to develop new treatments can also increase cybersecurity risks to the health care system.

Figure 3 Health Care Regulatory Visualization



However, to date there has been little focus on cybersecurity – while at the same time, the techniques being used by cyber criminals are growing increasingly sophisticated. According to a

recent KLAS[12] report, many survey respondents widely reported that their EHRs placed little attention on cybersecurity. Providers also report that many device manufacturers treat security as either an afterthought or that the attention is woefully inadequate.

Organizational Size Varies

The health care industry in the U.S. is a mosaic, which includes very large health systems, single physician practices, public and private payers, research institutions, medical device and software companies, and a diverse and widespread patient population. Today most health care is still delivered by smaller practices and rural hospitals that do not have the information security resources to implement protections against ongoing threats that change tactics and attack vectors quickly. These organizations often do not possess the infrastructure to identify and track threats, lack the technical capacity to analyze the threat data they receive in order to quickly translate it into actionable information, and lack capability to act on that information. Many of these organizations also lack physical and logical access controls consistent with best practices, continue to use unsupported legacy systems, and lack access to proper security training. In effect, these organizations have not crossed the cybersecurity digital divide. In some cases, larger health care organizations extend information security support to their affiliates and/or smaller local hospitals. Often affiliate sites lack sufficient IT resources and can be susceptible to security threats because they are part of the attack surface area. These risks and issues will continue to grow as the sophistication of attackers and attack vectors increases. A potential attack profile starts with the compromise of a smaller health delivery organization where the attacker increasingly exploits vulnerabilities until they acquire valid credentials necessary to gain access to a health information exchange and/or partner hospitals. While information security is often combined within IT budgets and remain flat or decrease each year because of competing priorities within the environment, the patient/industry is at great risk of a cyber attack that could seriously impact the safety of patients.

No organization has all the financial resources it needs to employ enough personnel necessary to consistently and confidently protect its networks and data. Many small organizations cannot afford to retain in-house information security personnel, or designate an IT staff member with cybersecurity expertise. A common, yet flawed, perception is that only large organizations are the target of cyber attackers due to the volume of sensitive, confidential, or proprietary information they possess. In reality, health care organizations of all sizes are targets due to the interconnected nature of the industry and all organizations face resource constraints. This is similar to a seemingly innocuous scrape on your leg that can lead to a systemic infection that jeopardizes your life.

Risks in Addition to Patient Care

Health care data is one of the rare types of personal data that one cannot change and has value that may increase over time. Credit card numbers, phone numbers, and bank account numbers can change when personal data is lost or otherwise compromised. Someone could steal a teenager's medical history today, only for it to become valuable when the individual achieves a

[12] A report generated by KLAS, an independently owned and operated US-based research company which conducts over 20,000 healthcare provider interviews/year, working with over 4,500 hospitals and over 3,000 doctor'soffices and clinics, rating over 250 healthcare technology vendors (e.g., radiology and laboratory vendors) a nd over 900products and services, and which publishes 40 performance and perception reports each year.

prominent role in public life. This difference in value is reflected in the price for medical records (vs. credit card numbers) available for sale on the dark web.[13] The general standard across many industries is to provide one-year of identity theft protection following a compromise of personnel or financial information. The identity protection is only a help for credit-based identity theft, it does not provide the patient with adequate protections based on the sensitivity, value, and permanence of their health care data, which is priceless.

Other risks include the potential for fraud (e.g., prescription medicines, insurance, Medicare and Medicaid), competitive disadvantage, brand damage, or stock manipulation based on vulnerabilities that are unknown to the public. For example, in 2016 an investment firm collaborated with "hackers" to uncover unknown security vulnerabilities in St. Jude Medical Inc.'s pacemakers and defibrillators.[14] This information allowed the firm to make strategic investment decisions and profit financially based on information that was unknown to the public or to St. Jude's.

The Complexity of Vulnerability Disclosure

In a 2014 White House blog post, Special Assistant to the President and Cybersecurity Coordinator Michael Daniel discussed publicly for the first time the question of "whether the federal government should ever withhold knowledge of a computer vulnerability from the public." In his post, he provided examples of when it might be appropriate for the government to withhold vulnerability information (i.e., to collect information for a law enforcement investigation). He revealed key principles of the decision-making process that the U.S. government goes through to determine whether or not to disclose newly discovered cybersecurity vulnerabilities.[15] This decision-making process, referred to as the Vulnerabilities Equities Process, has been controversial in the cybersecurity community,[16] and two major recent leaks indicate that the number of vulnerabilities that are withheld from public disclosure under this process are more substantial than some previously estimated.

The degree to which vulnerabilities should be withheld is a complex policy question for the entire cybersecurity community and is beyond the scope provided to this Task Force for examination.

With that said, the outsized impact of policy decisions on the health care industry and the resulting challenge to securing digital health systems is an important part of our task. Whenever U.S. government intelligence agencies choose to withhold a cybersecurity vulnerability from public disclosure, policy makers are taking a risk. This risk is not equally distributed among industries. In some cases, the health care industry will be impacted by the decision to withhold vulnerabilities to a much greater degree than other industries. For instance, the health care

[13] Farr, C. (2016, July). *On the Dark Web, Medical Records Are a Hot Commodity*. Retrieved from: Fast Company article regarding dark web and medical records
[14] Robertson, J. and Riley, M. (2016). *Carson Block's Attack on St. Jude Reveals a New Front in Hacking for Profit*. Retrieved from: Bloomberg news article regarding St. Jude attack
[15] Daniel, M. (2014). Heartbleed: *Understanding When We Disclose Cyber Vulnerabilities*. Retrieved from: Obama Whitehouse Archives
[16] Electronic Frontier Foundation (2016). EFF v. NSA, ODNI - Vulnerabilities FOIA. Retrieved from: ODNI Vulnerabilities

industry will likely see extensive adoption of WebRTC protocols[17] for use in video telemedicine. A future vulnerability in WebRTC might have an outsized impact on patient privacy as a result.

Further, specifically withholding vulnerabilities to medical devices or health care software might be interpreted as a violation of international treaties relating to perfidy (the portion of rules of warfare relating to good faith offerings of medical aid). As general purpose devices like cell phones become more commonly used as health care devices (i.e., with the addition of integrated heart rate monitoring or glucose tracking for instance) we believe that honoring the spirit and the letter of the law around this issue will become more complex.

III. Risks across the Health Care Industry

In 2015, HPH Sector experienced more cyber incidents resulting in data breaches than any of the other 15 critical infrastructure sectors.[18] Additionally, the rise and sophistication of ransomware attacks that hold IT systems and patient-critical devices hostage continues to grow, as evidenced by hospital ransomware attacks of 2016.[19,20] These incidents underscore the concerns about organizations having neither the awareness of current threats nor the technical personnel to prevent or deal with these threats, many of which are not new.[21] The increased focus on cybersecurity provides an opportunity for the health care industry to adapt and improve. The following sections describe the areas the Task Force highlighted in its discussions.

Distribution of Risks across the Health Care Value Chain

In an effort to gather additional information about risks to the confidentiality, availability, integrity of patient data, as well as to patient safety, the Task Force engaged in discussions with personnel from across the health care industry, including representatives from pharmaceutical companies, health plans and payers, medical device and equipment manufacturers, diagnostic testing centers, laboratories and patient service centers, providers, and health information and medical technology. The Task Force collected 151 potential risks across the value chain (68 confidentiality risks, 30 availability risks, 30 integrity risks, and 23 patient safety risks). See Figure 4 for a breakdown of identified risks by confidentiality, availability, integrity, and patient safety. Some identified risks relate to a single subsector or business process, while other risks are applicable across multiple subsectors and to multiple areas of the value chain. Of the risks identified, 55 percent related to the loss of PHI. Shared risks across the subsectors included the loss or modification of data, disruption of systems or processes, and asset loss or disruption due to software vulnerabilities. Note that the list of risks identified is not an exhaustive list to these subsectors, or to the entire health care industry. Further research should be conducted to identify a more comprehensive list of risks to share with the greater health care industry. Preliminary risks identified by the Task Force in a working document are available online.

---

[17] WebRTC Protocols. Retrieved from: Protocols

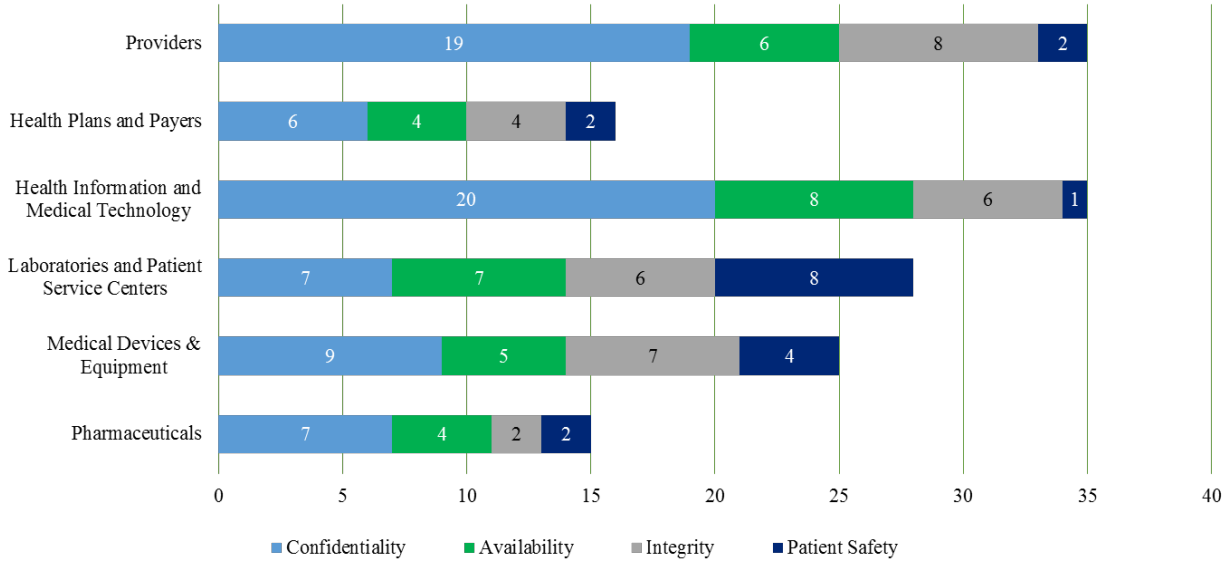
[18] Institute for Critical Infrastructure Technology. (2016). *Hacking Healthcare IT in 2016*. Retrieved from: ICIT brief on hacking healthcare IT

[19] Winton, R. (2016). *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*. Retrieved from: Los Angeles Times article on Hollywood hospital ransom

[20] Duncan, I. and McDaniels, A. (2016). *MedStar hack shows risks that come with electronic health records*. Retrieved from: MedStar hack shows risks

[21] Ponemon Institute. (2016). *The State of Cybersecurity in Healthcare Organizations in 2016*. Retrieved from: State of cybersecurity in healthcare by the Ponemon Institute

Figure 4 Health Care Subsector Risks across the Value Chain



Risks to Electronic Health Records

Regulatory mandates that will force all EHR vendors to have a shared, publicly-available application interface could expose EHRs to additional attack vectors. The goal has been, and should continue to be, for patients to be able to "use third party applications" to gain access to their health care data for improved service delivery. In light of these trends, HHS needs to consider the technical details of how to accomplish this level of interoperability in a secure manner prior to development and deployment. This will help ensure that this more universal access does not incidentally create a new vulnerable attack surface area.

The attack surface of the health information system expands when interconnected devices, such as mobile devices, medical devices, and applications, are permitted to connect to EHRs. Further complicating the health information system and EHR integration is the mobile device/application component. For simplicity, the EHR is the hub and connected medical devices are spokes. The modern EHR is the central exchange of the information super-highway that provides key clinical information and analytics to providers giving quality data, billing information, etc. Most deployed EHR solutions across the U.S. are built on more than one vendor's software solution. They are a complex mix of applications, programs, and interfaces from a variety of vendors. Implementing a patch, update, or significant data flow change requires massive support and a significant governance structure, which can destabilize the intricate and sometimes fragile connections to the "spokes". Conversely, medical device system changes and updates typically come from a manufacturer, which makes their software easier to change compared with changing EHR software. The National Cybersecurity and Communications Integration Center (NCIC) addressed this attack surface in their 2012 bulletin.[22] Though EHRs have some unique risks, the

[22] Department of Homeland Security. (2012). *Attack Surface: Healthcare and Public Health Sector*. Retrieved from: DHS NCCIC Medical Devices

risk to this technology is similar to medical devices as far as user and device authentication, timely updates, user access rights, risk of malware, and denial of service.

Risks to Networked Medical Devices and Connected IT Networks

This section explores the risks associated with the HPH subsectors and medical devices. All medical devices face a certain amount of cybersecurity risk. The risk of potential cybersecurity threats increases as more medical devices use software and are connected to the Internet, hospital networks, and other medical devices. This connectivity also improves health care and increases the ability of health care providers to treat patients. Because cybersecurity threats cannot be completely eliminated, manufacturers, hospitals, and facilities have to work to manage them to protect patient safety.

Cybersecurity threats and vulnerabilities can impact the confidentiality, availability, and integrity of IT networks and the medical devices and other systems connected to these networks. However, medical devices and the IT networks they connect to are unique. In addition to data security and privacy impacts, patients may be physically affected (i.e., illness, injury, death) by cybersecurity threats and vulnerabilities of medical devices. This harm may stem from the performance of the device itself, impeded hospital operations, or the inability to deliver care. As a result, addressing the patient safety risks posed by cyber threats are of paramount importance.

Table 1 below provides examples of cybersecurity risks that may relate to networked medical devices.[23,24,25,26] In Table 1, C = Confidentiality, I = Integrity, A = Availability, and PS = Patient Safety.

Table 1 Examples of Cybersecurity Risks to Networked Medical Devices and Connected IT networks

Risk Description	C	A	I	PS
Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices).	x	x	x	x
Malware which alters data on a diagnostic device.			x	x
Device reprogramming which alters device function (by unauthorized users, malware, etc.).	x	x	x	x
Denial of service attacks which make a device unavailable.		x		x
Exfiltration of patient data or PHI from the network.	x			

[23] FDA. (2013). *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*. Retrieved from: Cybersecurity for Medical Devices
[24] Deloitte. (2013). *Networked medical device cybersecurity and patient safety: Perspectives of health care information security executives*. Retrieved from: Cybersecurity and Patient Safety
[25] FDA. (2016). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: Management of cybersecurity in medical devices
[26] Storm, D. (2015). *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks.* ComputerWorld. Retrieved from: Hijacking medical devices

Risk Description	C	A	I	PS
Unauthorized access to the health care network, which allows access to other devices.	x	x	x	x
Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel).	x	x	x	x
Security vulnerabilities in off-the-shelf software due to poorly designed software security features.	x	x	x	x
Improper disposal of patient data or information, including test results or health records.	x			
Misconfigured networks or poor network security practices.	x	x	x	x
Open, unused communication ports on a device which allow for unauthorized, remote firmware downloads.	x	x	x	x

Risk Management Approaches

At a macro-level, organizations may leverage the NIST Cybersecurity Framework[27] (i.e., identify, protect, detect, respond, and recover) as a tool to help understand, manage, and communicate their cybersecurity risk. While the Framework provides a high-level description of standards and best practices to help organizations manage cybersecurity risks, it is not specific to the health care industry. Thus, the FDA provides industry specific guidance for medical device risk management through its pre- and postmarket guidance for management of medical device cybersecurity. These documents align to and overlay with the NIST Cybersecurity Framework.[28,29] Understanding the threats relevant to an organization is central to cybersecurity risk management. The Task Force realized the difficulty facing health care providers in creating processes and organizations that can quickly answer the question, "Does this threat information apply to me?" One approach is through voluntary sharing of threat information. Independent of this Task Force effort, ONC and ASPR provided grants and funding to support Information Sharing and Analysis Organization (ISAO) enhancements. These grants provide a foundation for some of our recommendations and allowed for the development of specific strategies and tactics that should make threat information sharing more effective.

Though FDA, ONC, and OCR guidance map to the NIST Cybersecurity Framework, implementing the framework remains a challenge. Industry-specific standards can help. For example, risk management is a shared responsibility and *IEC 8001: Application of risk*

[27] NIST. (2016). *NIST Cybersecurity Framework*. Retrieved from: NIST Cybersecurity Framework
[28] FDA. (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: Management of cybersecurity in medical devices
[29] FDA. (2016). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: Management of cybersecurity in medical devices

management for IT-networks incorporating medical devices defines the roles, responsibilities, and activities is associated with managing the risks within health care organization. In addition, organizational implementation is key and it is a challenge to implement these and other best practices. Risk management is a shared responsibility. Industry-specific standards such as *IEC 80001: Application of risk management for IT-networks incorporating medical devices* aids in this shared responsibility by helping health care organizations to define the roles, responsibilities, and activities associated with managing the risks of IT networks that incorporate medical devices. In addition to IEC 80001, FDA has also recognized several IT and security standards to aid medical device manufacturers.[30,31,32,33,34,35]

It is critical for stakeholders to develop a shared understanding of the risks posed by cybersecurity vulnerabilities and threats to medical devices and the IT networks to which these devices connect. Developing a shared understanding of risk assessments enables stakeholders to repeatedly and efficiently assess patient safety, public health, and security risks associated with cybersecurity vulnerabilities and threats. The Task Force identified several recommendations including recommended harmonization, Cybersecurity Framework standardization, and the creation of a secure development lifecycle as areas for sector improvement.

Security of the health information system is essential to the security of the sector at large. NIST published guidance around risks and best practices associated with accessing EHRs via mobile devices in NIST Special Publication 1800-1e DRAFT. The Task Force also discovered numerous requirements and best practices that can secure health information systems. See Appendix C – Resource Catalog for more information about publicly available resources.

[30] AAMI. (2015). *AAMI TIR57: Principles for medical device security—Risk management*. Retrieved from: Medical device security principles

[31] Clinical and Laboratory Standards Institute. (2014). *AUTO11-A2 - IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard*. Retrieved from: IT security of in vitro diagnostics

[32] ISO. (2012). *IEC/TR 80001-2-2:2012: Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls*. Retrieved from: Medical device security needs

[33] IEC. (2009).*Technical Specification 62443-1-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*. Retrieved from: Network security concepts and models

[34] IEC. (2010). *International Standard 62443-2-1 Edition 1.0 2010-11 - Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program*. Retrieved from: Security of industrial automation controls

[35] IEC. (2009). *Technical Report 62443-3-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems*. Retrieved from: Industrial communication networks

IV. Imperatives, Recommendations, and Action Items

Following a year of discussion within the Health Care Industry Cybersecurity Task Force (HCIC Task Force or Task Force) and information gathering from external stakeholders and subject matter experts across the health care industry and other sectors, the Task Force identified six imperatives that must be achieved to increase security within the health care industry. The Task Force conducted an in-depth examination of all topics identified in the *Cybersecurity Act of 2015* (the Act) Section 405's charge to the Task Force. The Task Force addresses these topics throughout this report and in the imperatives, recommendations, action items, and Appendices. The Task Force identified six high-level imperatives to organize the recommendations and action items. The imperatives are:

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT.
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
6. Improve information sharing of industry threats, risks, and mitigations.

Each imperative includes a set of recommendations and associated action items for implementing the recommendation. Recommendations contained within this report target the federal government, regulatory and legislative entities, health care industry stakeholders, and public-private partnerships. While some recommendations and action items identify a single entity to implement the actions, coordination across the public and private sectors will be critical to accomplishing these goals. Once implemented, the recommendations will help to increase awareness, manage threats, reduce risks and vulnerabilities, and implement protections not currently present across a majority of the health care industry.

While some recommendations are applicable to only certain health care subsectors, other recommendations have value for the entire industry. Although one could implement only a few of the recommendations and gain a minimal benefit, implementing all or a majority of the recommendations will compound the benefits to the overall security posture of the health care industry, as well as allow organizations to maximize their financial investments and personnel resources. See Appendix A for a summary of the imperatives, recommendations, and action items contained in this report.

Imperative 1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.

The health care industry in the United States (U.S.) is a mosaic, consisting of very large health systems, small/rural hospitals, single physician practices, public and private payers, research institutions, medical device and software companies, and a diverse and widespread patient population. Layered on this is a matrix of well-intentioned federal and state laws and regulations that can impede addressing issues across jurisdictions. This creates the potential to develop barriers to innovation and ease of use. Patients go for care based on their needs, not based on geographic boundaries. The industry has made great strides over the last 10 years in connecting the many stakeholders utilizing IT to improve health outcomes and create value through collaborative treatments. However, this vast electronic network needs to ensure privacy and security for all users, especially patients. The susceptibility of health care information to cyber threats has become very evident in the last few years with identity theft, ransomware, and targeted nation-state hacking becoming more frequent and extensive.

The complexity of the health care industry is enough to confound even relatively large organizations and their operations. The issues surrounding digital information exchange and providing appropriate security and privacy for that data represent a significant and urgent challenge.

Because there are multiple frameworks for addressing cyber risk, each organization tends to use a unique language and framework for determining risk. Use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework would standardize risk assessment and definitions to make sharing not only cyber information easier, but would allow the industry to understand the risk across the continuum of data. In addition to multiple frameworks, the industry struggles with federal legislation that can range from confusing to conflicting. Overlaying individual state and local laws can create additional areas of duplication or conflict. Therefore, the need for greater alignment and harmonization across all levels of government is absolutely necessary.

In health care, security and cyber risk has historically fallen to IT. Information governance is a relatively new concept in the industry and should include not just IT and security stakeholders, but also information stakeholders. Governance structures should also include clinical and non-clinical leaders. Governance of information shifts the focus from technology to people, processes, and the policies that generate, use, and manage the data and information required for care.

Finally, because of this complexity and the opportunities for confusion and conflict, there should be a single source for industry to go for authoritative clarification, explanation, and guidance. The Health Care Cybersecurity Leader (described in recommendation 1.1) would work within the Department of Health and Human Services (HHS), externally with other federal agencies that impact health care, and other health care sector-related groups to reduce duplication and provide guidance and clarity in the areas of security and cyber risk, best practices, education, and regulations.

The technical infrastructure underlying health systems is inordinately complex. It must support not only patient records but also a diverse suite of medical devices used in diagnosing, monitoring, and treating patients. Understanding and managing cybersecurity risks for this mission-critical environment is challenging as the health care system has a mixture of state-of-

the-art applications and devices, as well as older legacy devices that use unsupported operating systems or networking protocols. In addition, it is difficult to make these systems available for updates since they often provide round-the-clock care to patients to patients and cannot be taken out of service.

Health care organizations have, until recently, focused on meeting *Health Insurance Portability and Accountability Act* (HIPAA) privacy requirements by establishing and enforcing policies based on controlling access to protected health information (PHI). It is only recently, partly due to Meaningful Use security requirements, that health care organizations have begun to implement security management processes and safeguards as required by the HIPAA Security Rule. Cybersecurity issues, as recently demonstrated, require a more holistic view toward mitigating risk across the entire infrastructure. This demands a systematic approach for understanding, modeling and reducing risk, and compromise at multiple points in the infrastructure used to delivery care.

Recommendation 1.1: Create a cybersecurity leader role within HHS to align industry-facing efforts for health care cybersecurity.

Currently many different programs and agencies within and outside of HHS are responsible for health care industry cybersecurity. While it is appropriate that different HHS components have their own roles and responsibilities based on their legislative authorities, it is also important to have a single person who is responsible for coordinating these activities. The benefits of this coordination include:

- Allows one individual to look at cyber risks comprehensively, without being confined to specific program authorities, so that gaps can be more easily identified and addressed;
- Provides a single point of entry for health care industry partners to discuss cybersecurity concerns with HHS, so that they may be directed toward the appropriate points of contact without having to navigate a complex organizational structure;
- Helps prevent various components of HHS from engaging in conflicting or duplicative activities related to cybersecurity while promoting harmonization of regulations and guidance;
- Promotes consistent cyber incident response with industry;
- Enables HHS to advocate more effectively for health care cybersecurity as a whole;
- Allows HHS to leverage cyber expertise from multiple programs; and
- Ensures that Vulnerability Equities Processes, or any process that replaces it, takes the specific rules and implications of health care technology into account.

Action Item 1.1.1: *The HHS Secretary must name and resource a cybersecurity leader for sector engagement.*

Action Item 1.1.2: *The HHS Secretary must task the cybersecurity leader to work with federal, state, and industry partners to create a plan to establish goals and priorities for health care sector cybersecurity.*

Action Item 1.1.3: *The HHS Secretary must authorize the cybersecurity leader to define the reporting lines directly to other federal agencies tasked with cybersecurity such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and others.*

Action Item 1.1.4: *The cybersecurity leader must assist in streamlining HHS' outreach in a consistent manner to industry (e.g., branding, alignment with the NIST Cybersecurity Framework).*

Action Item 1.1.5: *The cybersecurity leader should establish a mechanism for partnering with and gathering industry input to prioritize short- and long-term goals, such as a federal advisory committee or similar mechanism.*

Action Item 1.1.6: *The cybersecurity leader should coordinate with U.S. and international intelligence agencies to ensure that Vulnerability Equities Process-like processes respect the special nature of digital health technology. Additionally, the cybersecurity leader should contribute to ongoing international policymaking and best practice development in this area.*

Recommendation 1.2: Establish a consistent, consensus-based health care-specific Cybersecurity Framework

As we observed in other critical infrastructure sectors, a framework helped establish a consensus-based standard for improving the conversation around cybersecurity. Although NIST has developed a generic framework, health care (like other sectors) has many unique aspects such as its diverse resource capabilities, legacy systems that will persist for years, and the burden of the need to have low barriers for sharing of data that is essential for collaborative patient-oriented care. The framework should build upon the minimum standard of security required by the NIST Cybersecurity Framework and the HIPAA Security Rule to promote a single lexicon for health care sector as well as standards, guidelines, and best practices. The complex environment requires certain basic standards that all stakeholders must meet and guidelines that allow flexibility for select issues. Without this framework, any of the countless constituents may pose a risk to the health care ecosystem.

Action Item 1.2.1: *HHS should complete work on the Act Section 405 (d) for Aligning Health Care Industry Security Approaches through a consensus-based approach to develop a health care sector specific cybersecurity framework.*

Action Item 1.2.2: *HHS and NIST must develop guidance about how to apply the framework to the health care sector.*

Action Item 1.2.3: *Industry and government should partner to establish an evaluation mechanism and prioritized best practices to support the range of small to large organizations to consistently apply the NIST Cybersecurity Framework.*

Recommendation 1.3: Require federal regulatory agencies to harmonize existing and future laws and regulations that affect health care industry cybersecurity.

The health care industry faces significant challenges due to federal and state cybersecurity laws and regulations that can be inconsistent and establish conflicting standards of compliance. These laws work in conjunction with laws on data breach notification, data disposal, and data security, often dictating different responses than federal laws. Additionally, complying with these laws and regulations is resource intensive and creates financial burdens for the health care ecosystem.

Because compliance with the various laws and regulations is burdensome, health care organizations often prioritize compliance over risk-based planning. A priority for regulatory agencies should be to ensure consistency among various federal and state cybersecurity regulations so that health care providers can focus on deploying their resources appropriately between securing patient information and the quality, safety, and accessibility of patient care instead of focusing on statutory and regulatory inconsistencies.

To demonstrate the complicated patchwork of laws, consider that in 2016, in addition to federal laws and regulations, members of the health care industry needed to adhere to computer crime laws touching upon issues such as:

- Unauthorized access, malware, and viruses in all 50 states;
- Denial of service attack laws in 25 states;
- Ransomware laws in two states, with another four states currently under consideration;
- Spyware laws in 20 states and two territories; and
- Phishing laws in 23 states and one territory.

Action Item 1.3.1: *HHS, in coordination with the private sector, federal, and state partners should look across HHS to harmonize regulations that directly or indirectly apply cybersecurity standards or best practices to reduce the burden on the industry.*

Action Item 1.3.2: *HHS should make recommendations to Congress about required statutory changes.*

Action Item 1.3.3: *HHS must publish standards and guidance consistent with the NIST Cybersecurity Framework. These should be developed based on the structure of the framework, as opposed to a mapping after the fact.*[36]

Action Item 1.3.4: *HHS should establish a Task Force to explore options to incentivize risk-based cybersecurity in alignment with their existing oversight roles.*

[36] Arias, A. (2016). *The NIST Cybersecurity Framework and the FTC*. Retrieved from: The NIST Cybersecurity Framework and the FTC

Action Item 1.3.5: *HHS should develop a conformity assessment model[37] built upon a public/private partnership to standardize cybersecurity compliance consistently across programs. Conformity assessments conducted by private sector organizations can increase productivity and efficiency and by encouraging federal agencies to standardize expectations.*

Recommendation 1.4: Identify scalable best practices for governance of cybersecurity across the health care industry.

Effective cybersecurity requires leadership at all levels of the organization. Not every organization is able to find, hire, and retain cybersecurity expertise. With small practices of only two to three people, the governance model looks vastly different from that of a multi-million dollar enterprise. Industry needs cybersecurity governance models that work for organizations of all sizes and provider types.

Governance is an issue of responsibility and authority, not specific cybersecurity expertise. Management of these organizations must be engaged in key activities that include: identifying, valuing, protecting, and managing assets and risks; establishing governance to include appropriate controls, training, processes, and procedures; and security incident response planning, readiness, and communications to ensure timely handling of and recovery from cyber events.

For example, while federal regulation calls for designated privacy and information security officers in covered entities, this has been done neither universally nor effectively across the health care industry. Changes in regulations designed to encourage health information sharing have also changed the relationship of the industry in relation to business associates; it is estimated that each covered entity has between four and 10,000 business associates.[38] This disparity in accountability and responsibility complicates and delays the effective and timely sharing of health information. Governance of, and responsibility for, cybersecurity can no longer be relegated to part-time positions or to individuals who have little training or expertise in the field.

Action Item 1.4.1: *Industry should establish scalable best practices for governance of cybersecurity across the health care industry.*

Action Item 1.4.2: *The health care industry should incorporate governance issues in the health care-specific Cybersecurity Framework discussed in Recommendation 1.2, and should commit to its adoption.*

[37] NIST. (2009). *Conformity Assessment*. Retrieved from: Conformity Assessment
[38] McGraw, D., Ingargiola, S., Wallis, K. *Business Associate Compliance With HIPAA*. Retrieved from: Compliance with HIPAA

Recommendation 1.5: Explore potential impacts to the Physician Self-Referral Law, the Anti-Kickback Statute, and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners.

The Task Force heard many concerns related to potential constraints imposed by the *Physician Self-Referral Law* (Stark Law) and the *Anti-Kickback Statute*. We strongly encourage Congress to evaluate an amendment to these laws specifically for cybersecurity software that would allow health care organizations the ability to assist physicians in the acquisition of this technology, through either donation or subsidy. A regulatory exception to the Stark Law and a safe harbor to the Anti-Kickback Statute to protect certain donations of electronic health records (EHR) effectively addresses management of technology between health care entities and serves as a perfect template for an analogous cybersecurity provision. Physician groups confront a myriad of financial challenges. Often these financial constraints limit their ability to manage the EHR software without trained security professionals who have the expertise to provide sufficient cybersecurity programs to protect their patient records. We need to empower small providers or suppliers (e.g., physician practices) to actively manage their security posture, not hinder them. Often organizations want to provide technology to ensure smaller business partners do not become a liability in the supply chain. An exception may provide for this assistance without creating fear of violating the Stark Law or Anti-Kickback Statute.

Further exacerbating the quagmire of federal and state laws, some regulatory agencies have strict liability standards in their evaluation of incidents. This means that even when the organization makes a reasonable and good faith effort to comply, it may still receive a regulatory fine or penalty, or be sued for damages. The HHS Office for Civil Rights is mandated to protect the privacy and security of PHI. The guidance states “protect against reasonably anticipated, impermissible uses or disclosures” and “reasonably anticipated threats or hazards.” In the current cyber environment, even the most robust health care entities cannot guarantee protection against all intruders. Sharing of information about security breaches is essential, but fear of penalties and bad publicity surrounding an event will often result in silence. The approach should be one of a just culture, now promulgated throughout health care. Mistakes and slips do not result in “discipline”, but reckless and negligent behavior does. This will promote transparency and improved protection of the global health care cyber environment.

Action Item 1.5.1: *Congress should explore potential impacts of the Physician Self-Referral Law and the Anti-Kickback Statute on collaborative industry cybersecurity efforts and identify potential modifications or exemptions as appropriate.*

Action Item 1.5.2: *Congress should establish a task force to make recommendations for harmonization of existing and future laws to remove the resource and financial burdens, such as those created by other fraud and abuse laws, and allow organizations to implement cybersecurity frameworks that will keep patients safe from cybersecurity threats.*

Imperative 2. Increase the security and resilience of medical devices and health IT.

The Health Care and Public Health (HPH) Sector is charged with keeping patients safe and that includes protecting patients and their information. This includes physical and privacy related harms that may stem from a cybersecurity vulnerability or exploit. If exploited, a vulnerability may result in medical device malfunction, disruption of health care services (including treatment interventions), and inappropriate access to patient information, or compromised EHR data integrity. Such outcomes could have a profound impact on patient care and safety. Some foundational challenges that will need to be addressed in order to enhance the cybersecurity of medical devices and EHRs include legacy operating systems, secure development lifecycle, strong authentication, and strategic and architectural approaches to product deployment, management, and maintenance on hospital networks.

The relatively short lifespan for operating systems and other relevant platforms such as commercial off the shelf software is inherently misaligned in health care as medical devices and EHRs may be utilized for 10, 15, 20, or more years. This misalignment may occur for a variety of reasons. Hospitals operate on thin budgets and cannot replace capital equipment like MRIs as quickly as new operating systems are released. Product vendors have a product development lifecycle that may take several years and they may start development using one operating system and by the time the product comes to market, newer operating systems may be available. Creative ways of addressing the aforementioned challenge areas may be found by engaging key clinical and cybersecurity stakeholders, including software vendors.

Recommendation 2.1: Secure legacy systems.

Legacy systems include both legacy medical devices and legacy EHR applications, which may not have any ongoing support from the hardware and software vendor(s) that provided these solutions. They may impact the entire system or system components, including firmware, drivers, operating systems, and all applications in use.[39,40] Many of these legacy systems have security weaknesses, which may contribute to the compromise of provider networks and systems. Every vendor and health care organization should be able to identify and classify legacy systems and develop an approach (e.g., compensating controls, device update, device retirement, network segmentation, or innovative architectures) to mitigate the associated risks. Note that though the action items below are provided within the context of legacy systems, **these action items are best practices** that should be adopted for all products, including new ones.

Action Item 2.1.1: *Health delivery organizations must: 1) inventory their clinical environments and document unsupported operating systems, devices, and EHR systems; 2) replace or upgrade systems with supported alternatives that have superior security controls where possible; 3) develop and document retirement timelines where devices cannot yet be replaced; and 4) leverage segmentation, isolation, hardening, and other compensating risk reduction strategies for the remainder of their use.*

[39] Note that there are several types of legacy products including legacy systems that are still supported by the product manufacturer, those that are not supported by the product manufacturer, and those that are supported by the product manufacturer but that have embedded software which is not supported by the software developer.
[40] Note that devices may be legacy but still have patches available.

Action Item 2.1.2: *Health care sector accreditation organizations (e.g., Joint Commission, and Centers for Medicare & Medicaid Services (CMS)) must: 1) consider incentives, requirements, and/or guidelines for reporting and/or use of unsupported system and mitigation strategies; and 2) develop aggressive timelines for conformance.*

Action Item 2.1.3: *For devices that still receive some support from the device manufacturer and/or application vendor, these organizations must make real-time updates and patches (e.g., to the operating system), as well as make compensating controls available to end users. Organizations should also have a policy/plan in place to be able to receive and implement available updates.*

Action Item 2.1.4: *Government and industry should develop incentive recommendations to phase-out legacy and insecure health care technologies (e.g., incentive models like Cash for Clunkers,[41] Montreal Protocol,[42] and Federal IT Modernization Fund[43]). As a part of looking at incentives, government and industry should create partnerships/alliances to establish roadmaps for joint enhancement of cybersecurity interoperability and maturity through better procurement processes.*

Recommendation 2.2: Improve manufacturing and development transparency among developers and users.

In order to track medical device vulnerabilities, there is a need for transparency regarding third party software components. Having a "bill of materials" is key for organizations to manage their assets because they must first understand what they have on their systems before determining whether these technologies are impacted by a given threat or vulnerability. Moreover, this transparency enables health care providers to assess the risk of medical devices on their networks, confirm components are assessed against the same cybersecurity baseline requirements as the medical device, and implement mitigation strategies when patches are not available. To date, this practice has not been widely adopted.

Product vendors should be transparent about their ability to patch and update products during the procurement process, including the timeline for end of device support. This includes relaying to potential customers the amount of time remaining for product support during procurement. Additionally, health delivery organizations should ensure that their systems, policies, and processes account for the implementation of available updates and patches.

Action Item 2.2.1: *Manufacturers and developers must create a "bill of materials" that describes its components (e.g., equipment, software, open source, materials), as well as any known risks associated with those components to enable health care delivery organizations to more quickly determine if they are impacted.*

[41] Department of Transportation – National Highway Traffic Safety Administration. (2016). *Car Allowance Rebate System (CARS) – Transactions.* Retrieved from: DOT
[42] Multilateral Fund. *Montreal Protocol*. Retrieved from: Multilateral Fund
[43] Information Technology Modernization Act. (2016). Retrieved from: U.S. Congress

Action Item 2.2.2: *Industry should actively participate in information sharing programs to better recognize and manage cybersecurity vulnerabilities and threats.*

Action Item 2.2.3: *Industry (e.g., manufacturers, vulnerability finders, etc.) must adopt and engage in coordinated vulnerability disclosure consistent with recognized standards (e.g., ISO/IEC 29147and ISO/IEC 30111[44]).*

Recommendation 2.3: Increase adoption and rigor of the secure development lifecycle (SDL) in the development of medical devices and EHRs.

Manufacturers should manage security risks within their product risk management processes including safety risk management, and consider risks throughout the lifecycle (from concept generation through end of life recycling or disposal) and across all levels of the system supply chain. If any one of these lifecycle phases or system levels is left unaddressed, that represents a potential susceptibility to cyber-related risks.[45] Testing and/or certification may help to provide assurance that safety and security have been considered for all phases of the lifecycle. The desired end state is to identify security requirements at the earliest possible stages of the lifecycle to help ensure security and privacy by design, rather than as an afterthought. These processes would help to manage and eliminate security weaknesses in the system. They would also communicate the dispositioning of such weaknesses and the identification of new security flaws to all appropriate stakeholders, enabling responsibility agreements[46] and policies that would help to provide the necessary security and privacy assurances. Taken together, SDL activities would help to reduce safety risks, which is of paramount importance in protecting patients.[47]

Industry can leverage government guidance and industry standards. NIST Special Publication (SP) 800-160 provides guidance on engineering-driven practices to develop defensible systems.[48] Food and Drug Administration (FDA) has also provided guidance[49] to medical device manufacturers regarding cybersecurity and risk management concerning the incorporation of commercial off the shelf software. Premarket[50] and postmarket[51] management guidance recommendations issued by the FDA advocate that manufacturers should monitor, identify, and

[44] International Organization for Standardization. (2013). *ISO/IEC 30111:2013. Information technology -- Security techniques – Vulnerability handling processes*. Retrieved from: Information technology -- Security techniques -- Vulnerability handling processes

[45] NIST. (2008). *NIST Special Publication 800-64 Revision 2: Security Considerations in the System Development. Life Cycle*. Retrieved from: Security considerations in SDLC

[46] ISO. (2010). *IEC 80001-1:2010 Standard*. Retrieved from: ISO IEC80001

[47] Rispoli, D., Brasil, L., Rispoli, V., Fernandes, P. (2013). *Software Lifecycle Activities to Improve Security Into Medical Device Applications*. Retrieved from: Improving security in medical device applications

[48] NIST. (2016).*NIST Special Publication 800-160 - Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Retrieved from: NIST Systems Security Engineering

[49] FDA. (1999). *Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices*. Retrieved from: FDA reviewers and compliance for medical device software

[50] FDA. (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: Premarket submissions for medical device cybersecurity

[51] FDA. (2016). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: Postmarket submissions for medical device cybersecurity

address cybersecurity vulnerabilities and exploits as part of the SDL. Industry standards for assurance requirements for medical devices include AAMI TIR 57, UL 2900,[52] and DTSec's[53] cyber security standards initiative.

Action Item 2.3.1: *Manufacturers, developers, and users should implement security by design throughout the product lifecycle, including operations and maintenance.*

Action Item 2.3.2: *Manufacturers and developers should plan for operations and maintenance to ensure continuous monitoring, ongoing patching, and weakness remediation.*

Action Item 2.3.3: *Industry must include threat modeling as a clear part of their SDL including their system development lifecycle (SDLC). Industry should recognize, characterize, and manage weaknesses relative to common attack patterns and evolving threats, ideally during design and development of the technology or post hoc in the form of compensating controls within the broader system environment into which the technology would be integrated.*

Action Item 2.3.4: *Manufacturers should better leverage and attest to mature standards for secure product lifecycle including secure SDLC across design, development, manufacturing, service, support, and through end of life.*

Action Item 2.3.5: *Industry should develop processes for assessing risks for integrated systems that cross regulatory boundaries, such as EHRs and medical devices.*

Action Item 2.3.6: *Industry should develop recommendations for incorporating patient safety and clinical hazards into the Common Vulnerability Scoring System (CVSS) for better risk management.*[54]

Action Item 2.3.7: *Manufacturers should provide instructions for secure configuration of devices on networks, documentation on secure preparation for recycling and disposal of medical devices, and specific guidance regarding supporting infrastructure architecture (e.g., network segmentation requirements). Ideally these instructions would include how to scrub any personally identifiable information, PHI, or other site-specific sensitive data such as configuration files.*

Action Item 2.3.8: *Industry and government should consider issuing a grand challenge, soliciting from stakeholders novel incentive structures that could be leveraged to address cybersecurity challenges specific to securing legacy systems, SDL, strategic and architectural approaches, and holistic data flow and system requirements for EHRs (e.g., creating a challenge which develops or identifies reference architectures and operating systems for safety critical systems which are higher assurance, more interoperable, and supported for longer periods of time).*

---

[52] UL. (2016). *UL Launches Cybersecurity Assurance Program*. Retrieved from: UL cybersecurity assurance program

[53] Diabetes Technology Society. (2016). *New Standard to Raise Confidence in the Security of Network-Connected Medical Devices through Expert Evaluation*. Retrieved from: Evaluation of network connected medical devices

[54] FIRST. (2015). *Common Vulnerability Scoring System, V3 Development Update*. Retrieved from: Vulnerability Scoring System

Action Item 2.3.9: *Government agencies (e.g., FDA and HHS Office of the National Coordinator for Health Information Technology) should consider how they can use their existing authorities to catalyze and reinforce activities and action items associated with this recommendation. Areas of interest may include unsupported operating systems, hardcoded passwords, tactical guidance related to evolving threats like botnets or ransomware, etc.*

Recommendation 2.4: Require strong authentication to improve identity and access management for health care workers, patients, and medical devices/EHRs.

The delivery of health care is founded on the establishment of a trust relationship between and among providers and patients. The foundation of this trust is the belief and confidence in the identities of the individuals involved (providers and patients). Through strong identity and access management practices, this trust relationship should be extended to the medical devices that are used to provide patient care.

Clinicians in a hospital setting are required to access multiple computers throughout the facility repeatedly (up to 70 times per shift) as they deliver care to patients. In order to authenticate their identity so that they can perform common tasks (e.g., access a patient's medical record, order diagnostic tests, prescribe medication, etc.), a clinician typically enters his or her user name and a unique password. This widely used, single factor approach to accessing information is particularly prone to cyber attack as such passwords can be weak, stolen, and are vulnerable to external phishing attacks, malware, and social engineering threats. NIST SP 800-63[55] adopts alternatives to the use of passwords for user authentication, including items in the user's possession (e.g., a proximity card or token) or biometrics. Clinicians also interact with medical devices and the integrity of the devices used in these treatments must be assured from a bioengineering and a cybersecurity perspective. The provider operating the device must be authenticated and authorized to operate it, and the patient needs to be accurately identified as the person authorized to receive the treatment. Moreover, communications between the device and other health care technologies should be authenticated (i.e., devices should know what technologies they are communicating with and should only be communicating with technologies with the appropriate credentials).

Just as the need to authenticate providers is critical to the establishment of the trust relationship in the delivery of health care, it is also becoming more important that patients accessing electronic information be properly identified and authenticated. Patient access to health care services requires the same level of confidence in establishing rights to access or modify medical records, to schedule appointments, and to receive care. Additionally, promoting the use of multi-factor authentication, leveraging biometrics, and mobile phones and/or wearables can help to establish a trust relationship with the patient.

The Task Force believes that the implementation of policies and processes in health care that are consistent with Recommendation 1.3 of the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital Economy*, including the elimination of passwords as

[55] NIST. (2013). *NIST Special Publication 800-63-2: Electronic Authentication Guideline*. Retrieved from: NIST electronic adjudication guidelines

the means for accessing clinical information systems, will allow providers and patients to maintain this trust relationship for the foreseeable future.

Action Item 2.4.1: *Until a national standard exists, health care stakeholders should work collaboratively to establish standards for device-device authentication such that interoperability is not impeded.*

Action Item 2.4.2: *In situations where the provider is accessing an EHR or Health Information Exchange external to the hospital or clinical environment, the health care industry should adopt the NIST SP 800-46 guidelines for remote access including the use of two-factor authentication to ensure a compromised password cannot alone be used to gain access.*

Recommendation 2.5: Employ strategic and architectural approaches to reduce the attack surface for medical devices, EHRs, and the interfaces between these products.

Industry needs to take a long-range approach to considering viability, effectiveness, security, and maintainability of those products when setting up the IT network and at the outset of product deployment. The desired end-state is that every product (whether new or when it is being upgraded) have a defined strategy, architectural approach, and design that supports the deployment and overall lifecycle management of that product.

Action Item 2.5.1: *Manufacturers should focus on architecturally supporting security interoperability for their products that validate, and leverage health care delivery organizations existing security controls.*

Action Item 2.5.2: *Industry should establish a task force to collaborate on issues related to risks and challenges of product interdependencies and two-way data flows. These interdependencies include medical devices, EHRs, Internet of Things (IoT), and two-way data flows.*

Action Item 2.5.3: *HHS should evaluate existing authorities and identify gaps to conduct cybersecurity surveillance of medical devices and EHRs.*

Action Item 2.5.4: *Industry should build and anticipate the need for IT forensics to accompany adverse event investigations by ensuring that logs exist and are accessible.*

Action Item 2.5.5: *Health care providers should ensure collaboration among department leadership, biomedical engineering teams, IT staff, and IT security in the selection, deployment, and maintenance of medical devices.*

Recommendation 2.6: Establish a Medical Computer Emergency Readiness Team (MedCERT) to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures.

In the interest of national security, there is a need for a MedCERT that focuses on medical devices because of the inherent impacts to patient safety when vulnerabilities are disclosed and/or exploited. The medical device-specific MedCERT would have a broad range of expertise (including hardware, software, networking, biomedical engineering, and clinical) that will enable it to understand the patient safety implications of incidents and vulnerabilities, and comprehensively coordinate responses. As a part of its vulnerability disclosure function, this team would help to assess vulnerabilities, evaluate any patient safety risks, serve as an adjudicator between the vulnerability finder and the product manufacturer, assess proposed mitigations, and serve in a consultation role for organizations navigating the coordinated vulnerability process. The team's responsibilities regarding evaluation and assessment during an exploit would be similar except there would be the added functionality of a "go-team" that could be deployed in the field to investigate a suspected or confirmed device compromise.

Action Item 2.6.1: *Federal agencies must partner with industry to define the scope and scale of a MedCERT. The MedCERT would be a trusted entity that is viewed as independent and neutral by all stakeholders and will work to arrive at "the ground truth" of vulnerabilities and proposed mitigations.*

Action Item 2.6.2: *In order to validate the vulnerabilities and impacts, as well as assess the public fixes (mitigations and patches), the MedCERT will need to rely upon the technical analyses provided by independent certification and testing capabilities. These technical analyses provided by individual testing labs will need to be correlated to support the MedCERT's vulnerability validation and assessment roles.*

Imperative 3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.

Every sector faces challenges in meeting its need to recruit and retain qualified cybersecurity professionals. The health care industry in particular is experiencing a large growth in IT adoption, which will continue to exacerbate the challenge. Rather than discussing universal cyber workforce problems, the following recommendations are tailored to the unique challenges facing the health care industry.

These challenges include:

- Identifying people and tools for addressing the small and medium-size health care organizations which cannot typically afford full-time technical resources. A two-person dental office or independent home health care provider cannot establish a fully resourced cybersecurity office that is necessary to stay ahead of cyber threats. Leveraging shared service providers and secure solutions may be options for some organizations.

- Limited resources with tight profit margins for reinvestment into cybersecurity, particularly in the small and medium-sized organizations. Balancing the procurement of medical supplies (e.g., ambulances, x-ray machines) with improved security technologies will continue to be a trade-off.

- Identifying cybersecurity leadership roles to help identify risks, as well as to prioritize and advocate for resources.

- Growing patient involvement in their care increases exposure to threats. This introduces an enormous potential vulnerability as patients want electronic access to their medical records, yet often do not use good cybersecurity best practices. In addition, consumers are extremely worried about identity theft, including financial and now health information.

Recommendation 3.1: Every organization must identify the cybersecurity leadership role for driving for more robust cybersecurity policies, processes, and functions with clear engagement from executives.

Accountability and responsibility for cybersecurity in an organization is often poorly defined and many health care organizations view cybersecurity as an IT problem. Organizations need to identify a cybersecurity leader to drive change. In many organizations, this may be the Chief Information Security Officer (CISO) role; however, in smaller organizations this is often a collateral duty.

Most health care organizations today would benefit from sufficient leadership and resources to help ensure that cybersecurity requirements are identified, prioritized, fulfilled, and maintained. Such resources would address business needs as well as regulatory mandates. In order to provide effective leadership over information and cybersecurity functions, health care organizations should identify a CISO or other officially designated individual that serves as the most senior information and cybersecurity professional. At a minimum, this individual should be responsible

for ensuring an appropriate corporate security program is established and enforced within this complex environment.

For many health care organizations, it may not be feasible to have a CISO or team of personnel dedicated exclusively or primarily to cybersecurity matters. However, it is important that these organizations designate a specific individual to provide leadership and prioritize risks pertaining to cybersecurity initiatives and issues. This individual must have both the authority, as well as the appropriate expertise to carry out such responsibilities. For example, in many organizations, a full-time dedicated resource for this role may not be feasible; in such instances, the organization should assign an individual to the CISO/security leader role as an official component of their broader role and may leverage resources as part of a managed service provider or consultants. In some cases, the CISO/security leader role may also include overall authority and responsibility for privacy matters. In such instances, the privacy component of the role should be officially documented and designated.

Action Item 3.1.1: *Industry should establish best practices for the qualifications and governance models that support the cybersecurity and privacy leadership role within their organizations.*

Action Item 3.1.2: *Industry should establish governance structures to empower CISOs to express risks and advocate for resources with organizational leadership.*

Action Item 3.1.3: *Industry should identify opportunities for defining shared or third party CISO roles for small organizations.*

Recommendation 3.2: Establish a model for adequately resourcing the cybersecurity workforce with qualified individuals.

Nationwide, there is a deficit of cybersecurity talent across all industries. Many small, medium, and rural health care organizations have few qualified, dedicated security resources available. The prospect of supplying even one dedicated resource per organization currently looks daunting; however, managed services and contracted external resources/partners can enhance cybersecurity capability and services.

California started the first safe patient ratio staffing system for registered nurses. This program evolved from a critical need to protect patients, nurses, and health delivery organizations. We find ourselves in a similar situation regarding cybersecurity. There is a need to determine a similar acceptable ratio of health care cybersecurity expertise to the size of the organization, complexity of care, degree of interconnectedness with other organizations, etc. The larger the organization, the more security professionals are required. This ensures workload balancing across the organization to better protect the organization, clinicians, and most importantly the patients.

Currently, it is difficult to ensure workforce competencies due to the number of certification programs that are not all tailored to the health care environment. A simple search of the Internet yields hundreds of “cybersecurity” degrees across the nation and around the world. While there are many valid degrees, the rigors, depth of knowledge, and competencies vary from program to program. Immediately, there needs to be a method for certifying higher education programs in cybersecurity, particularly focusing on health care and patient safety.

The foundation of this recommendation is the certification of higher education programs. Certification of these degree-awarding programs assures students and future employers a core competency to best defend the health care industry. The workforce produced by these certified cybersecurity programs, if started in 2017, would not be able to join the workforce at a novice level until 2021.

At this time, the Task Force looked at multiple approaches to address the immediate gap and many of these are discussed in other recommendations in this report to include:

- Examining the impacts of the Stark Law[56] and Anti-Kickback[57] regulations;
- Leveraging managed security service providers (MSSPs) to develop a business and security model; and
- Utilizing MSSPs to provide a platform to grow the future cybersecurity professional workforce.

Action Item 3.2.1: *Industry should develop a research report, similar to the California Safe Patient Ratio, to identify appropriate voluntary benchmarks for cybersecurity staffing per patient accounting for various exceptions/factors (e.g., research centers/academic medical centers/ambulatory versus inpatient facilities).*

Action Item 3.2.2: *HHS should consider options[58], in coordination with industry partners, to develop a conformity assessment program to establish standards for different roles within the health care industry and authorize education providers against those standards.*

Action Item 3.2.3: *Organizations such as the Committee on National Security Systems (CNSS), the National Centers of Academic Excellence in Cyber Defense (CAE-CD), DHS, or NIST should consider establishing mechanisms to assist in developing the requirements for and certifying advanced degree cybersecurity programs.*

Action Item 3.2.4: *Industry should define mechanisms to educate and better leverage clinicians, in a tiered workforce model, capable of fundamental cybersecurity-related tasks.*

Action Item 3.2.5: *Congress should provide financial support to CNSS and CAE-CD for cybersecurity education certification to ensure core competencies for health care cybersecurity professionals.*

Action Item 3.2.6: *Industry and the federal government should explore opportunities for individuals to engage in ongoing internship programs to develop more information security professionals in supporting the health care industry.*

---

[56] Stark Law. (2013). *Stark Law*. Retrieved from: Stark Law

[57] The American Health Lawyers Association. (2005). *Anti-Kickback Statute*. Retrieved from: Anti-Kickback Statute

[58] As a starting point, the cybersecurity workforce taxonomy is provided in the NICE Cybersecurity Workforce Framework (NIST SP 800-181) NICE cybersecurity framework. The NICE taxonomy could be the foundational standard against which a conformity program was applied.

Recommendation 3.3: Create MSSP models to support small and medium-size health care providers

Currently, the majority of small and medium-size health care providers, non-profit providers, clinicians, and rural hospitals face a significant struggle in hiring the appropriate level of information security personnel to support a "healthy" cybersecurity posture. Individually these entities may not hold as many EHR records as their larger counterparts, but they are just as vital to their patients. A coordinated attack on multiple small and medium-size health care providers could pose a significant risk to national security. Breaches of small and medium-size health care providers, both possible and realized, destabilize public trust in the health care industry and as such, negatively affect the entire critical infrastructure sector. These entities are also an easy target for cyber threats.

We recommend that industry create more low-cost, MSSP models to support these smaller and under-funded entities in order to ensure that they have the same level of robust, state-of-the-art security monitoring, defensive, and reporting capabilities as larger health care organizations. This would allow health care organizations to leverage resources and expertise, such as a shared security official, and will create economies of scale. MSSPs would be better resourced to engage in information sharing activities, such as Information Sharing and Analysis Organizations (ISAO). Since smaller entities usually have less complex systems and the MSSPs would help standardize and develop efficient and cost-effective support mechanisms for small and medium-size organizations. The MSSPs should focus on critical network perimeter controls, end-point controls, identity and access management, and encryption; they should also develop a reasonable cyber hygiene program to establish ongoing security monitoring and maintenance, as well as articulate security controls against the Cybersecurity Framework.

Action Item 3.3.1: *The federal government should evaluate incentive options, such as grants and tax incentives, to encourage more MSSPs to achieve economies of scale to support small and medium-size health care providers.*

Action Item 3.3.2: *Federal regulatory agencies should evaluate incentive options, such as crediting small and medium-size health care providers who have engaged MSSPs during their audits and breach investigations, to encourage providers to leverage MSSPs.*

Action Item 3.3.3: *Industry and the federal government should explore opportunities for individuals to engage in ongoing internship programs (e.g., at MSSPs and federal agencies) to develop more information security professionals in supporting the health care industry.*

Recommendation 3.4: Small and medium-sized health care providers should evaluate options to migrate patient records and legacy systems to secure environments (e.g., hosted, cloud, shared computer environments).

Small and medium-sized health care providers continue to maintain local servers and databases, often in closets or in unsecure infrastructure. In addition to the workforce limitations, a majority of these health care providers still have legacy EHR systems, aging infrastructure, poor disaster recovery capabilities, and capital investment limitations.

One method for achieving a more secure environment may be cloud computing. Hosted cloud service providers and hosting companies (ranging from the vendors themselves to larger health care systems) have made significant advancements in security controls and technologies. These approaches may operate on a lower-cost model than an organization building everything itself; these models can be an appealing, cost-effective, and feasible alternative for many small and medium-size health care organizations. In fact, some major cloud service providers and EHR vendors already market secure cloud computing environments that may align with HIPAA requirements. By moving to a secure cloud environment, health care providers will have increased security and the ability to effectively use their clinical resources to support patients without having to worry about maintaining their on-premises infrastructure and systems. Organizations that leverage these models should remain cognizant that moving their data or system to another environment or physical location does not remove all security obligations from the organization. The organization must also understand that this becomes an issue of shared responsibilities with all parties responsible for overall security, including appropriate legal and Business Associate Agreements.

Action Item 3.4.1: *The federal government should evaluate incentive options, such as grants, to encourage industry to develop secure options for supporting small and medium-size health care organizations.*

Action Item 3.4.2: *The federal government should evaluate incentive options, such as tax incentives, to encourage health care providers migrate to more secure environments including hosted services (i.e., vendors or other providers) or cloud service providers.*

Action Item 3.4.3: *Federal regulatory agencies should provide additional guidance to service providers (including HHS-compliant Business Associate Agreements) that wish to align their security management practices with HIPAA and create increased awareness among health care providers that alternative technologies exist to store, access, share, and process their data.*

Action Item 3.4.4: *Industry should develop use cases and contracts tailored for these small and medium-size organizations.*

Action Item 3.4.5: *Insurance companies should provide more incentives to encourage small and medium-size health care service providers who migrate to a more secure environment than the one in which they currently operate.*

Imperative 4. Increase health care industry readiness through improved cybersecurity awareness and education.

Cybersecurity can be an enabler for the health care industry, supporting both its business and clinical objectives, as well as facilitating the delivery of efficient, high-quality patient care. However, this requires a holistic cybersecurity strategy. Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients.

Cybersecurity must be governed with a collaborative approach whereby all members of the health care industry work together toward the common goal of protecting one another and the sector's most critical assets – patients. To achieve this requires an educated workforce and an informed public who make evidence-based decisions that are reliant on cyber-secure data. As part of this holistic security strategy, it is critical that a thorough baseline is established whereby inherent trust can be established between patients and providers, technologies and processes, and ultimately institutions and patients.

This will lead to a high level of confidence in which the industry understands cybersecurity hygiene and ultimately establishes trust throughout the health care continuum. Once a baseline level of hygiene is established, the industry must come together to develop a methodology to audit, measure, and continually steer the industry progressively forward.

The health care industry must increase outreach for cybersecurity across all members of the health care workforce through ongoing workshops, meetings, conferences, and tabletop exercises. Additionally, the health care industry must provide patients with information on how to manage their health care data by developing consumer grading systems for non-regulated health care services and products. Lastly, the health care industry must develop cyber literacy programs to educate decision makers, executives, and boards of directors about the importance of cybersecurity education.

Recommendation 4.1: Develop executive education programs targeting Executives and Boards of Directors about the importance of cybersecurity education.

Developing an education campaign will help Executives and members of the Boards of Directors to gain increased awareness and understanding of the value of cybersecurity initiatives and funding. By understanding the threats and risks to the organization, efforts can be made to help ensure these threats and risks are mitigated and/or managed in such a manner that supports the mission and future viability of the organization. As advocates for organizational resources, IT leadership is neither well prepared nor well equipped to communicate cybersecurity risks and investment needs that could help to protect the organization and the patients they serve. To create this national education program and campaign, it is recommended that existing federal cyber awareness campaigns (e.g., DHS Stop.Think.Connect and Federal Trade Commission (FTC) OnGuard Online) and resources be utilized to create consistent messaging; to be on trend with current messaging; and to also create foundational, specific, and actionable tips and takeaways for each stakeholder group.

Action Item 4.1.1: *Trade and professional associations should ensure cyber workforce training and education focuses on corporate officers and Boards of Directors communication.*

Action Item 4.1.2: *Trade and professional associations in the health care industry should develop materials for CISOs and security leaders to better communicate with executive level leadership and Boards of Directors regarding security risks, priorities, and cyber hygiene posture.*

Action Item 4.1.3: *Health care organizations should participate in National Cybersecurity Awareness Month events in their area and become partners of the National Cybersecurity Awareness Campaign, managed through DHS as a baseline to build and customize for the HPH Sector.*

Recommendation 4.2: Establish a cybersecurity hygiene posture within the health care industry to ensure existing and new products/systems risks are managed in a secure and sustainable fashion.

The awareness of cybersecurity risks and threats are inconsistently understood when making both personal and organizational decisions regarding cybersecurity. The health care-specific cybersecurity framework, discussed earlier, will help establish common language and terminology.

Cybersecurity hygiene refers to an individual's "health" (or security) when conducting activities online. Cybersecurity hygiene equates to personal hygiene in that it is the individual's responsibility; it includes all online behaviors and implementing practices such as creating strong passwords, running virus and security scans, and backing up personal data. The deployment of a cybersecurity hygiene baseline establishes the minimum practices that every person and organization should perform. This applies to both industry and to patients.

Action Item 4.2.1: *Industry should manage all health care infrastructure technology (including IoT) security to focus on patient safety, both on an individual and population basis, with an appreciation of how the technology will be used and how it could be misused.*

Action Item 4.2.2: *Industry should ensure that no known malware exists in newly produced equipment/software entering the market (i.e., premarket), and there should be ongoing surveillance for malware in equipment/software currently in the market (i.e., postmarket).*

Action Item 4.2.3: *Health care organizations must develop a strategy for cybersecurity hygiene for existing and legacy equipment, a systematic approach for patching, implementation of compensating controls, isolation, and/or replacement (as available or applicable) should be applied. For newly produced equipment/software entering the market, device manufacturers should have a plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device.*[59]

[59] FDA. (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Retrieved from: FDA Content of Premarket submissions

Recommendation 4.3: Establish a conformity assessment model for evaluating cybersecurity hygiene that regulatory agencies and industry could rely on, instead of a diversity of auditors.

Conformity assessment in this context is the determination that a given network connectable technology repeatedly and reproducibly satisfies a standardized set of basic cybersecurity requirements. Implementing a public-private conformity assessment model would standardize the requirements for basic cybersecurity hygiene across health care regulatory bodies and reduce the financial burden on affected industry. Conformity assessments would establish accredited entities in the private sector to reduce the overall regulatory burden to: 1) regulators themselves in terms of their capacity, 2) technology vendors in terms of improving their time to market, and 3) to health care providers who seek to adopt the technologies as rapidly as possible while maintaining patient safety and security.

Conformity with the cybersecurity baseline requirements can be demonstrated through mechanisms such as public certificates or certification markings on a product (analogous to having voltage, current, and frequency markings on the back of most certified electrical products). This can demonstrate that the cybersecurity hygiene baseline has been met, which reduces the need for regulators, vendors, and providers to provide their own individual assessments of conformity to this common set of baseline cybersecurity requirements. Different stakeholders need to validate, test, and certify against the baseline throughout the lifecycle (including during system development, procurement, deployment, and maintenance). The existing maintenance mechanisms of certification (e.g., postmarket surveillance, adverse event monitoring, and remediation) can be used to keep the cybersecurity posture of products reasonably current throughout the product lifecycle (following established industry norms including those for safety-critical software quality).

While all of these elements and action items of the baseline for cybersecurity hygiene are desirable, their implementation should take into account economics, time-to-market for new technologies, and workforce capability/capacity (an effort likely requiring some level of public-private partnership). To build such marketplace capabilities, establishing a living body of knowledge to define key elements of the cybersecurity hygiene baseline is another important construct. Demonstrating technical competency in such a body of knowledge, to provide verification to the marketplace that the baseline requirements have been satisfied, can be managed through many different models of accreditation currently available to coordinate between the public and private sector.

One such model in the U.S. is the Nationally Recognized Test Lab model administrated by Occupational Safety and Health Administration. A similar model used across the international community is the International Electrotechnical Commission's System of Conformity Assessment Schemes for Electrotechnical Equipment and Components and Common Criteria for Information Technology Security Evaluation an international standard (ISO/IEC 15408) that provides a framework for specifying security, functional, and assurance requirements that independent testing laboratories can evaluate products against.

This can be accomplished by creating a scheme that relies upon using industry-recognized standards within the existing ecosystem of private sector standards developers, accreditors, certification organizations, testing organizations, technology vendors, and technology consumers to comprise a new ecosystem that delivers against this baseline of cybersecurity hygiene. Given

the complexity of interconnected clinical environments, multiple testing organizations with different sets of expertise and laboratory resources may be needed to validate products against multiple standards to fully assess conformance to the baseline. These organizations should be able to operate in a federated manner and combine their results to facilitate organizational risk assessments. Such a model has the potential to expedite market adoption of safe, secure, and innovative new health care technologies that can improve upon the current state of security in this part of our nation's critical infrastructure.

Action Item 4.3.1: *Health care regulatory agencies in partnership with industry should establish the requirements for a common set of requirements upon which the conformity assessment program would be built.*

Action Item 4.3.2: *The federal government should resource and establish a process for the oversight of the conformity assessment program.*

Action Item 4.3.3: *Health care regulatory agencies should develop strategies to begin to phase in certifiers who have been accredited under the conformity assessment program.*

Action Item 4.3.4: *The federal government in coordination with industry should develop a business model/incentives to ensure that the testing, validation, and certification data is widely available to health care providers, regardless of size and resources.*

Action Item 4.3.5: *Health care regulatory agencies should be familiar and continue to build upon the National Cybersecurity Workforce Framework[60] for an understanding of cybersecurity roles, responsibilities, and the knowledge, skills, and abilities required for each cybersecurity role. The Workforce Framework is available at Workforce Framework.*

Recommendation 4.4: The NIST Baldrige Cybersecurity Excellence Builder, should be further developed: 1) specific to health care, and 2) specific to the types of health care operations that are widely deployed across the industry and have limited access to cybersecurity resources (e.g., small hospitals or practices, rural locations with limited access to security resources).

The Task Force noted that Covered Entities have been required to perform a HIPAA Security Risk Assessment since 2005 when the Security Rule went into effect. Information security was a new concept to health care at that time. Digitization and automation were just beginning to be widely adopted into health care practice, and technology platforms, such as cloud and mobile computing, were not in broad use. Issues of security were focused on technical security, not operational impacts or risks to patient care. Consequently, the Office for Civil Rights has repeatedly cited the incompleteness of risk assessments (e.g., failure to perform risk assessments, failure to use the risk assessments that were done to build a response plan and mitigate identified risks) in their enforcement activity.

NIST recently published a self-assessment tool, the NIST Baldrige Cybersecurity Excellence Builder, that companies and other organizations can use to assess the effectiveness of their

[60] DHS. *National Cybersecurity Workforce Framework*. Retrieved from: NICCS

cybersecurity risk management efforts. This self-assessment tool, developed in collaboration with industry, blends the organizational performance evaluation strategies from the Baldrige Performance Excellence Program and the risk management mechanisms of the NIST Cybersecurity Framework. The document was designed to help specialists explain the importance of cybersecurity to the company's bottom line. However, it does not address health care specific risks such as patient care impacts from cyber events or medical devices.

The document was aimed at two constituencies: cybersecurity specialists within an organization and, more generally, business executives that run the mission and operations. These are the people that need to understand why and how cybersecurity is important to the organization. For the cybersecurity specialists, this self-assessment will help them articulate cybersecurity's impact on the company's operations and finances. Business executives or clinicians will begin to understand how cybersecurity affects the processes and business of health care.

Tailoring this tool to the health care industry would also assist the industry in shifting the security perspective from one focused on compliance to one that emphasizes risk management.

Action Item 4.4.1: *HHS and NIST should develop a health care specific version of the NIST Baldridge Cybersecurity Excellence Builder.*

Action Item 4.4.2: *HHS and NIST should develop a tiered version of the tool for the industry based on size and business model (e.g., physician practice, clinic, hospital, Academic Medical Center, business associates).*

Action Item 4.4.3: *In order to establish an industry-wide baseline, the self-assessment should be required for all Covered Entities while granting exemption or partial exemption to fines or prosecution as a result of that assessment and corrective action plans.*

Recommendation 4.5: Increase outreach and engagement for cybersecurity across federal, state, local, tribal, territorial, and the private sector partners through an education campaign including meetings, conferences, workshops, and tabletop exercises across regions and industry.

The susceptibility to cyber threats exists for many organizations because most people are neither aware of the risks, nor have the tools to protect their systems. Cybersecurity is a shared responsibility that requires diligence from all who interact with or facilitate the collection, maintenance, and exchange of health care information and use interconnected medical systems. Poor cybersecurity practices at any level can become the cause of a breach and leave patients exposed to unexpected harm to their privacy or even the care they receive.

There is currently a lack of shared awareness of cybersecurity risks and best practices among health care systems. The health care sector should engage with HHS and DHS to build on the established National Cybersecurity Awareness Campaign to ensure broad outreach to the sector and develop a baseline cybersecurity understanding at all levels, as well as tailored information for health care executives, clinical providers, patients, and other key groups that may not possess fluency in IT matters. This awareness will provide them the ability to use health care IT in a risk-informed manner so they can take the necessary steps to better protect health care information.

A national education program should be developed specifically for health care users who do not have a high degree of cybersecurity awareness. Although there are multiple education seminars available, there needs to be a standardized program that serves as a baseline for all. There should be several arms – one for providers and clinicians, one for administrators, and one for non-provider daily users, such as registrars. In order to ensure that the program is meaningful and will address the needs, a pre-course survey would help provide information to define the knowledge gap so the program will be appropriately structured and can be constantly updated.

Action Item 4.5.1: *HHS should work with government and industry partners to develop an outreach and engagement campaign to increase health care cybersecurity awareness and literacy among health care providers, patients, and IT professionals.*

Action Item 4.5.2: *HHS should work with government and industry partners to develop a specific outreach program for health care executives, so that they can have a better understanding of the importance of cybersecurity in their own organizations and can better engage with cybersecurity professionals to ensure that protective programs are adequately managed and resourced.*

Action Item 4.5.3: *HHS should work with government and industry partners to develop a series of workshops to explore current questions in health care cybersecurity, such as evaluation of best practices, research and development (R&D) needs, and the role of insurance.*

Action Item 4.5.4: *HHS should work with government and industry partners to develop educational materials for patients to assist them in accessing, managing, and protecting their health care information.*

Action Item 4.5.5: *HHS should work with government and industry partners to develop a national health care cyber-literacy course that is updated on a biannual basis to keep up with rapidly changing technology and to train health care professionals on the importance of cybersecurity in their day-to-day tasks. Industry at all levels should incorporate principles from this course into all patient education modules or courses, as applicable.*

Action Item 4.5.6: *HHS should work with government and industry partners to develop a health care mentoring program to help educate non-IT staff to proper risk management of IT and information sharing.*

Action Item 4.5.7: *HHS should identify privacy experts, patient advocates, regulatory experts, and proprietary information experts to discuss issues related to fraud or stock manipulation.*

Recommendation 4.6: Provide patients with information on how to manage their health care data, including a cybersecurity and privacy grading system for consumers to make educated decisions when selecting services or products around non-regulated health care services and products.

Today, people experience near-universal dependence on IT and information exchange for all aspects of daily life. Most individuals are unsure about how to protect their data and personal information. Their uncertainty is heightened when patients are at their most vulnerable. Since

health care data is generated from a variety of sources, and not just from the traditional provider settings, specialized training and information should be provided about privacy and security related to health care information, patient rights, and health information collected outside of traditional provider environments. This covers topics ranging from federal and state regulations related to patient information, to social media, to wearable devices ranging from fitness trackers to medical devices, to medico-legal issues around providers having timely and accurate patient information.[61]

Increasingly health care is shifting toward consumer devices and applications that may or may not fall within existing regulations. Implementing a product evaluation process, such as *Consumer Reports* or a "housekeeping seal of approval" to independently assess and rate consumer health care/lifestyle products will help to educate consumers when selecting and using products that are subject to cybersecurity risks and handle privacy data. This concept helps to promote industry innovation within a safe and secure framework.

Action Item 4.6.1: *The FTC should engage health care and consumer organizations to develop a process to evaluate, assess, and rate health care/lifestyle products. This aligns to action item 3.1.3 of the Commission on Enhancing National Cybersecurity's Report on Securing and Growing the Digital Economy.*

Action Item 4.6.2: *HHS, DHS, NIST, and FTC should establish a grant or national challenge for a consumer grading system.*

[61] Rock Health. (2016). *2016 Year End Funding Report: A reality check for digital health*. Retrieved from: Rockhealth: Digital health

Imperative 5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.

The health care sector is consistently one of the biggest investors in R&D across the U.S. In 2015, a total of $158.7 billion[62] the sector invested in health care R&D. $102 billion (or 64 percent) of this investment came from private industry[63] including pharmaceutical manufacturers, life sciences, and medical device manufacturers. Another $36 billion came from the federal government and accounted for more than half of the federal government's non-Department of Defense R&D spend.[64]

While the primary goals of these investments are to develop life-saving therapies and products, this massive R&D investment has significant direct and indirect economic impacts across the nation. For example, the biopharmaceutical industry alone employed 810,000 people and supported another 1,022,000 million indirect jobs.[65] National Institutes of Health funding and grants provided over $32 billion[66] to more than 2,500 academic and medical research entities and helped to support about 300,000 scientists in their medical research. These well-paying and stable jobs[67] help fuel the economy in cities and towns across the U.S.

This massive investment in R&D also creates an increasingly lucrative target for intellectual property and trade secret theft. This threat is particularly prominent from countries that are looking to significantly improve their own health care R&D capacity. For example, China recently began implementation of its 13th Five-Year Plan for Economic and Social Development of the People's Republic of China. This plan highlights the need to develop China's internal biotech industry, build its high-performance medical equipment capabilities, and grow its advanced manufacturing capacity.[68] The plan also stresses the need make broad and deep reforms across the health care industry including R&D. Unfortunately, over the last few years there have been a number of cases involving attempted intellectual property theft by Chinese entities using both physical and cyber methods;[69,70,71,72] this was prior to the added pressure of milestones and objectives that will stem from the 13th Five-Year Plan.

This Task Force, seeing the threat to the greater financial and intellectual security of the nation, outlines the following recommendations and action items to better secure R&D and intellectual property, which directly tie to the U.S. economy.

---

[62] Research America. (2016). *U.S. Investments in Medical and Health Research and Development*. Retrieved from: US investments in medical and health R&D
[63] Ibid.
[64] AAAS. (2016). *Federal R&D in the FY 2016 Budget: An Overview*. Retrieved from: FY 2016 Budget overview
[65] PhRMA. (2015). *2015 Profile: Biopharmaceutical Research Industry*. Retrieved from: 2015 profile of biopharma
[66] National Institutes of Health. (2017). *Budget*. Retrieved from: NIH budget
[67] Ibid. In 2011, the average total compensation per direct biopharmaceutical employee was $110,490, twice the average compensation per US worker of $54,455.
[68] People's Republic of China. (2016). *The 13th Five-Year Plan For Economic and Social Development of the People's Republic of China*. Retrieved from: People's Republic of China 13th five year plan
[69] United States District Court for the Eastern District of Pennsylvania. Retrieved from: GlaxoSmithKline case in US District Court for Eastern District of Pennsylvania
[70] PlainSite. (2014). *Indiana Southern District Court, Case No. 1:13-cr-00150*. Retrieved from: USA versus CAO
[71] Shanghai Pudong New District People's Court, Criminal Division, First Instance Judgment No. 1616 of 2012.
[72] Pink Sheet. (2014). *Novartis Sues Former Researcher In China For Alleged Trade Secret Theft*. Retrieved from: Novartis sues former researcher in China

Recommendation 5.1: Develop guidance for industry and academia on creating economic impact analysis and loss for cybersecurity risk for health care research and development.

Develop guidance on evaluating the potential economic impact, reputational damage, loss of intellectual property, and other cybersecurity risks for health care R&D. The lack of clear and consistent guidance results in industry and academia undervaluing the risk to the health care industry. Provide the resources to more adequately evaluate the risk when an organization's leadership resources IT and cybersecurity. Creating this evaluation will help organizations to better value their data assets when evaluating and applying security resources.

Action Item 5.1.1: *The federal government should work with industry to establish a task force to develop risk models for evaluating U.S. economic and organizational impact for cybersecurity failures.*

Action Item 5.1.2: *Industry should develop best practices to balance academic freedom, intellectual property, and health care services.*

Action Item 5.1.3: *HHS should partner with the DHS Science and Technology Directorate to identify grand challenges, priorities, and implement new research to support small and rural organizations.*

Action Item 5.1.4: *Congress should identify resources for improving research addressing small and rural provider security challenges.*

Action Item 5.1.5: *HHS should partner with DHS and Office of the Director of National Intelligence to identify specific threat actors and the techniques that they employ to target U.S. health care R&D information. This information should be updated regularly to stay abreast of emerging tactics and techniques.*

Action Item 5.1.6: *HHS should present findings from Action Item 5.1.5 to senior executives and other representatives from the R&D industry.*

Recommendation 5.2: Pursue research into protecting health care big data sets.

Big data in the health care industry presents a unique set of challenges due to the size, valuable insights, and the volume of patient data handled by these systems. A majority of academic health care institutions, as well as medium and large size health care providers, have already established some form of big data solutions. In addition, there are big data solutions and initiatives managed by non-profit and state government entities. Malicious users and state sponsored terrorists have an incentive to focus on these big data solutions as they could cause significant damage to these organizations and also result in the theft of millions of records and intellectual property from a small number of systems.

Action Item 5.2.1: *Entities that manage big data solutions should ensure that a detailed risk assessment is performed at frequent intervals and that they address 100 percent of preventative security controls, including continuous monitoring programs to mitigate inappropriate access.*

Action Item 5.2.2: *Entities that manage big data solutions should have detailed documentation of source and destination connections and diligent review and approval process in managing these connections.*

Action Item 5.2.3: *Entities that manage big data solutions should apply minimum necessary security principles in providing users/organizations with access to these systems to mitigate disastrous situations with these systems.*

Action Item 5.2.4: *Health care providers should exercise solid due diligence processes when selecting third party solutions or cloud-based solutions, as well as ensure that sufficient administrative safeguards are in place, including an unlimited indemnification clause in case of data breaches.*

Action Item 5.2.5: *Entities that manage big data solutions should apply extreme care in determining what data is collected, what data is retained, and what data is deleted as more data presents increased security risks.*

Imperative 6. Improve information sharing of industry threats, risks, and mitigations.

The passage of the *Cybersecurity Act of 2015* helped strengthen the information sharing partnership between the federal government the private sector across all industries. In particular, Title 1 provided for the establishment of systems to improve the automated sharing of cyber threat indicators in near real time. The Act charged the Task Force to develop a plan for federal government and industry stakeholders to implement Title 1 within the health care sector.

There are unique challenges to implementing an information sharing system in the health care industry. Data-sharing approaches are often successful for organizations that already have the resources, personnel, and infrastructure to analyze large volumes of technical information. However, a large portion of the health care industry is either a small or medium sized business. With one or fewer dedicated cybersecurity experts on staff, small and medium-size organizations can rarely leverage or take advantage of this constant stream of information. In some instances, this volume of information can become overwhelming. In addition, there is no single entity within the health care industry that is currently resourced to provide a comprehensive information sharing solution to the entire industry.

During the course of the year's discussion, the Task Force heard from a wide array of government and industry stakeholders that are currently involved in health care cybersecurity information sharing. Through these discussions, the Task Force gained an appreciation for the large number of stakeholders involved, their diverse information needs and ability to consume data, and the often complex legal issues involved in the sharing of certain types of information. They heard from information sharing organizations of all types, including those in the federal government, and those in the private sector. They heard from both not-for-profit and for-profit organizations.

It became clear that in order to develop the most effective information sharing system, HHS and the health care industry should take a flexible approach, engaging closely with the many information sharing initiatives currently underway as they grow and evolve. Together, industry and government should work together to ensure that the best resources are leveraged from the various systems and tailored toward the unique needs of health care while protecting privacy and maintaining appropriate legal protections. The Task Force provides the following principles for guiding these efforts, in addition to the more specific recommendations that follow.

- All health care industry stakeholders – including health care organizations of all sizes – should have the opportunity to engage in the process of building the health care industry's information sharing system.

- Existing systems – both governmental and private sector – should be leveraged to the greatest extent possible.

- Systems should leverage all available tools for addressing liability and other legal issues involved in information sharing, including those provided under the Act Title I.

- The health care industry's approach should build upon and align with cross-sector information sharing activities, including those coordinated through DHS.

- While there is a role for proprietary information sharing approaches, at least a baseline level of information must be made available to organizations of all sizes and level of resources without additional charge.

- Any information sharing plan should take into account the significant challenges that lower resourced organizations often have in consuming and analyzing cybersecurity information streams. Information should be made available in multiple formats, tailored toward different levels of organizational capability.

- The information sharing approach should be implemented in a manner that is consistent with the protection of civil rights, civil liberties, privacy, and the protection of proprietary information.

Recommendation 6.1: Tailor information sharing for easier consumption by small and medium-size organizations who rely on limited or part-time security staff.

Understanding the large quantity of information sharing data, regulatory complexities, and existing cyber hygiene maturity is overwhelming for small and medium-size organizations. The information and guidance needs to be streamlined for quick and efficient consumption. A diversity of information threat feeds is not practical to consume for an organization that only has personnel that are responsible for cybersecurity as a collateral duty. Even for large organizations that consume various industry threat feeds, the volume, differing formats, and consolidating of incoming data can be burdensome.

In addition, a lot of potential data regarding threats and risks is lost because small providers do not have a mechanism for sharing information with the ISAOs. Leveraging MSSPs could help to provide a better picture of the industry attack surface.

Action Item 6.1.1: *HHS in cooperation with the ISAOs should streamline and consolidate information sharing data on threats whenever practical for easier consumer adoption.*

Action Item 6.1.2: *Industry should incentivize the adoption of information sharing for small and medium-sized organizations for MSSPs.*

Recommendation 6.2: Broaden the scope and depth of information sharing across the health care industry and create more effective mechanisms for disseminating and utilizing data.

The concept of Information Sharing and Analysis Centers was first introduced in 1998 during the Clinton Administration through *Presidential Decision Directive 63 – Critical Infrastructure Protection*. That directive strongly encouraged critical infrastructure entities to share information about any threats, vulnerabilities, and incidents that have the potential to disrupt or degrade the continuity of any critical infrastructure component. Subsequent Administrations and Congress have strongly endorsed this concept and codified the support through statutes, Presidential Directives and Executive Orders. For example, the *Homeland Security Act of 2002* recognized ISAOs as a category of information sharing organizations broader than the Information Sharing

and Analysis Centers. In 2015, Congress passed the Act to address concerns about liability and privacy issues that might hinder the adoption of this concept by industry.

The Task Force identified several limitations, highlighted with the action items, with the existing ISAO approach, which could be improved to help protect the sector.

Action Item 6.2.1: *HHS in coordination with ISAOs should evaluate incorporating hazards (e.g., national disasters, acts of terrorism, pandemic outbreaks) with the potential to disrupt critical health infrastructure in their information sharing threat analysis.*

Action Item 6.2.2: *HHS should work with all federal partners to ensure that intelligence reports and threat information is consolidated and given additional context as distributed to industry.*

Action Item 6.2.3: *HHS should partner with industry to identify health care subsector priorities for intelligence reporting. For example, payers may be extremely interested in information regarding medical insurance fraud and emerging cybercrime tactics that are used to support this activity, whereas pharmaceutical companies are likely to be very interested in the changing methods used by nation state actors to steal intellectual property.*

Action Item 6.2.4: *HHS and the ISAO should continue to work with DHS and other entities to develop processes for quickly curating and releasing critical threat information.*

Recommendation 6.3: Encourage annual readiness exercises by the health care industry.

Current planning and practices for a cyber incident readiness are often insufficient within health care, and a significant event could produce an uncoordinated and ineffective response. According to various published studies, more than 70 percent of firms surveyed stated that they have incident response plans in place, yet less than 15 percent of these organizations review or exercise their plans annually.[73] Incident response plans that are not regularly reviewed or tested put the health care industry at risk. Response to cybersecurity incidents within health care should be planned and tested as other serious incidents that can affect health care, such as fast-spreading viruses or prescription drug contamination.

Generic critical infrastructure response plans already exist and are in use by organizations in other industries. These response plans could be used to create tailored plans for the health care industry. Organizations should conduct exercises regularly to test these plans and to create and utilize a variety of relevant incident scenarios. The response plans and exercises need to be representative of the complexity of the health care industry and account for the interaction of many subsectors. They should also incorporate scenarios that include regional, national, and global attacks. Exercises should also address the difficulties to respond due to the convergence of information technologies and physical systems. In addition, clear operating authority should be outlined and guidance given on where the private sector should go for information and assistance from the federal government.

[73] Ponemon Institute. (2014). *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness*. Retrieved from: The Second Annual Study on Data Breach Preparedness
SANS Institute. (2014). *Incident Response: How to fight back*. Retrieved from: SANS Institute on Incident response
HITRUST. (2015). *Breach Response: What's the Plan?*

Action Item 6.3.1: *HHS and industry should identify those critical incident response plans that could be best leveraged by the health care industry.*

Action Item 6.3.2: *Industry should implement cybersecurity incident response plans, which are reviewed and tested annually.*

Action Item 6.3.3: *HHS, DHS National Cybersecurity and Communications Integration Center (NCIC), and law enforcement should maintain unified and dedicated channels during steady state and response efforts to: 1) provide subject matter expertise to issues that involve the HPH Sector; 2) leverage existing sector relationships across government, within industry, and with an impacted entity; and 3) facilitate targeted dissemination, clarification, and near real-time notifications to the health care industry in a strategically sequenced manner.*

Recommendation 6.4: Provide security clearances for members of the health care community.

HHS currently leverages the DHS Private Sector Clearance Program to provide security clearances for health care industry partners who have a need to know classified information. These clearances are provided within the structure of the HPH Sector Critical Infrastructure Protection Partnership to provide early access to threat information for data which is not yet declassified for the public. Due to the cost involved in the application process and ongoing maintenance for a security clearance, it is impossible for all health care industry partners to be granted a security clearance. However, it is important to establish mechanisms for prioritizing clearances for those organizations with the greatest ability to act on cyber threat information to reduce cyber risks to the nation's health care system.

Action Item 6.4.1: *HHS, DHS, and the FBI should review the HPH Sector's utilization of the Private Sector Clearance Program to identify gaps and strengthen the criteria and process through which health care industry partners can apply for clearances.*

V. Future Considerations

The public-private partnership developed by the Task Force and resulting in this report has been a valuable opportunity to address significant concerns for cybersecurity in the health care industry. The conversations with industry associations and partners made clear the priority that industry places on cybersecurity at this time. However, the Task Force identified future opportunities that others may wish to pursue.

- Develop a cohesive plan for implementing the report recommendations and develop appropriate metrics to measure implementation progress.

- Conduct a risk analysis, similar to the National Infrastructure Protection Plan, with an overlay for health care cybersecurity and privacy. Based upon the analysis, develop a comprehensive cybersecurity roadmap for the HPH Sector.

- Establish an ongoing public-private forum, similar to this Task Force, to further the discussions of health care industry cybersecurity as the industry evolves. The Task Force members found this engagement with federal partners beneficial to understand our common cybersecurity challenges and concerns.

- HHS leadership should partner more closely with existing DHS efforts with the insurance industry in helping identify a roadmap to enable private insurance approaches in the health care industry. The sometimes-conflicting roles of HHS as a regulatory body and facilitator for improved security could be mitigated by encouraging an industry-based insurance market.

- Enable an ongoing conversation and develop strategies to identify resources and incentives that would help to overcome the barriers faced by small and rural organizations.

Appendix A: Imperatives, Recommendations, and Action Items

The following tables document the imperatives, recommendations, and action items contained in this report.

Imperative 1	**Define and streamline leadership, governance, and expectations for health care industry cybersecurity.**
Recommendation 1.1	**Create a cybersecurity leader role within the Department of Health and Human Services (HHS) to align industry-facing efforts for health care cybersecurity.**
Action Item 1.1.1	The HHS Secretary must name and resource a cybersecurity leader for sector engagement.
Action Item 1.1.2	The HHS Secretary must task the cybersecurity leader to work with federal, state, and industry partners to create a plan to establish goals and priorities for health care sector cybersecurity.
Action Item 1.1.3	The HHS Secretary must authorize the cybersecurity leader to define the reporting lines directly to other federal agencies tasked with cybersecurity such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and others.
Action Item 1.1.4	The cybersecurity leader must assist in streamlining HHS' outreach in a consistent manner to industry (e.g., branding, alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework).
Action Item 1.1.5	The cybersecurity leader should establish a mechanism for partnering with and gathering industry input to prioritize short- and long term goals, such as a federal advisory committee or similar mechanism.
Action Item 1.1.6	The cybersecurity leader should coordinate with United States (U.S.) and international intelligence agencies to ensure that Vulnerability Equities Process-like processes respect the special nature of digital health technology. Additionally, the cybersecurity leader should contribute to ongoing international policymaking and best practice development in this area.
Recommendation 1.2	**Establish a consistent, consensus based health care specific Cybersecurity Framework.**
Action Item 1.2.1	HHS should complete work on the Act Section 405 (d) for Aligning Health Care Industry Security Approaches through a consensus-based approach to develop a health care sector specific cybersecurity framework.
Action Item 1.2.2	HHS and NIST must develop guidance about how to apply the framework to the health care sector.
Action Item 1.2.3	Industry and government should partner to establish an evaluation mechanism and prioritized best practices to support the range of small to large organizations to consistently apply the NIST Cybersecurity Framework.

Imperative 1	Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
Recommendation 1.3	**Require federal regulatory agencies to harmonize existing and future laws and regulations that affect health care industry cybersecurity.**
Action Item 1.3.1	HHS, in coordination with the private sector, federal, and state partners should look across HHS to harmonize regulations that directly or indirectly apply cybersecurity standards or best practices to reduce the burden on the industry.
Action Item 1.3.2	HHS should make recommendations to Congress about required statutory changes.
Action Item 1.3.3	HHS must publish standards and guidance consistent with the NIST Cybersecurity Framework. These should be developed based on the structure of the framework, as opposed to a mapping after the fact.
Action Item 1.3.4	HHS should establish a Task Force to explore options to incentivize risk-based cybersecurity in alignment with their existing oversight roles.
Action Item 1.3.5	HHS should develop a conformity assessment model built upon a public/private partnership to standardize cybersecurity compliance consistently across programs. Conformity assessments conducted by private sector organizations can increase productivity and efficiency and by encouraging federal agencies to standardize expectations.
Recommendation 1.4	**Identify scalable best practices for governance of cybersecurity across the health care industry.**
Action Item 1.4.1	Industry should establish scalable best practices for governance of cybersecurity across the health care industry.
Action Item 1.4.2	The health care industry should incorporate governance issues in the health care-specific Cybersecurity Framework discussed in Recommendation 1.2, and should commit to its adoption.
Recommendation 1.5	**Explore potential impacts to the Physician Self-Referral Law, the Anti-Kickback Statute, and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners.**
Action Item 1.5.1	Congress should explore potential impacts of the Physician Self-Referral Law and the Anti-Kickback Statute on collaborative industry cybersecurity efforts and identify potential modifications or exemptions as appropriate.
Action Item 1.5.2	Congress should establish a task force to make recommendations for harmonization of existing and future laws to remove the resource and financial burdens, such as those created by other fraud and abuse laws, and allow organizations to implement cybersecurity frameworks that will keep patients safe from cybersecurity threats.

Imperative 2	Increase the security and resilience of medical devices and health IT.
Recommendation 2.1	**Secure legacy systems.**
Action Item 2.1.1	Health delivery organizations must: 1) inventory their clinical environments and document unsupported operating systems, devices, and electronic health record (EHR) systems; 2) replace or upgrade systems with supported alternatives that have superior security controls where possible; 3) develop and document retirement timelines where devices cannot yet be replaced; and 4) leverage segmentation, isolation, hardening, and other compensating risk reduction strategies for the remainder of their use.
Action Item 2.1.2	Health care sector accreditation organizations (e.g., Joint Commission, and Centers for Medicare & Medicaid Services (CMS)) must: 1) consider incentives, requirements, and/or guidelines for reporting and/or use of unsupported system and mitigation strategies; and 2) develop aggressive timelines for conformance.
Action Item 2.1.3	For devices that still receive some support from the device manufacturer and/or application vendor, these organizations must make real time updates and patches (e.g., to the operating system, etc.), as well as make compensating controls available to end users. Organizations should also have a policy/plan in place to be able to receive and implement available updates.
Action Item 2.1.4	Government and industry should develop incentive recommendations to phase-out legacy and insecure health care technologies (e.g., incentive models like Cash for Clunkers, Montreal Protocol, and Federal IT Modernization Fund). As a part of looking at incentives, government and industry should create partnerships/alliances to establish roadmaps for joint enhancement of cybersecurity interoperability and maturity through better procurement processes.
Recommendation 2.2	**Improve manufacturing and development transparency among developers and users.**
Action Item 2.2.1	Manufacturers and developers must create a “bill of materials” that describes its components (e.g., equipment, software, open source, materials), as well as any known risks associated with those components to enable health care delivery organizations to more quickly determine if they are impacted.
Action Item 2.2.2	Industry should actively participate in information sharing programs to better recognize and manage cybersecurity vulnerabilities and threats.
Action Item 2.2.3	Industry (e.g., manufacturers, vulnerability finders, etc.) must adopt and engage in coordinated vulnerability disclosure consistent with recognized standards (e.g., ISO/IEC 29147and ISO/IEC 30111).
Recommendation 2.3	**Increase adoption and rigor of the secure development lifecycle (SDL) in the development of medical devices and EHRs.**
Action Item 2.3.1	Manufacturers, developers, and users should implement security by design throughout the product lifecycle, including operations and maintenance.
Action Item 2.3.2	Manufacturers and developers should plan for operations and maintenance to ensure continuous monitoring, ongoing patching, and weakness remediation.

Imperative 2	Increase the security and resilience of medical devices and health IT.
Action Item 2.3.3	Industry must include threat modeling as a clear part of their SDL including their system development lifecycle (SDLC). Industry should recognize, characterize, and manage weaknesses relative to common attack patterns and evolving threats, ideally during design and development of the technology or post hoc in the form of compensating controls within the broader system environment into which the technology would be integrated.
Action Item 2.3.4	Manufacturers should better leverage and attest to mature standards for secure product lifecycle including secure SDLC across design, development, manufacturing, service, support, and through end of life.
Action Item 2.3.5	Industry should develop processes for assessing risks for integrated systems that cross regulatory boundaries, such as EHRs and medical devices.
Action Item 2.3.6	Industry should develop recommendations for incorporating patient safety and clinical hazards into the Common Vulnerability Scoring System for better risk management.
Action Item 2.3.7	Manufacturers should provide instructions for secure configuration of devices on networks, documentation on secure preparation for recycling and disposal of medical devices, and specific guidance regarding supporting infrastructure architecture (e.g., network segmentation requirements). Ideally these instructions would include how to scrub any personally identifiable information, protected health information (PHI), or other site specific sensitive data such as configuration files).
Action Item 2.3.8	Industry and government should consider issuing a grand challenge, soliciting from stakeholders novel incentive structures that could be leveraged to address cybersecurity challenges specific to securing legacy systems, SDL, strategic and architectural approaches, and holistic data flow and system requirements for EHRs (e.g., creating a challenge which develops or identifies reference architectures and operating systems for safety critical systems which are higher assurance, more interoperable, and supported for longer periods of time).
Action Item 2.3.9	Government agencies (e.g., the Food and Drug Administration (FDA) and HHS Office of the National Coordinator for Health Information Technology) should consider how they can use their existing authorities to catalyze and reinforce activities and action items associated with this recommendation. Areas of interest may include unsupported operating systems, hardcoded passwords, tactical guidance related to evolving threats like botnets or ransomware, etc.
Recommendation 2.4	**Require strong authentication to improve identity and access management for health care workers, patients, and medical devices/ EHRs.**
Action Item 2.4.1	Until a national standard exists, health care stakeholders should work collaboratively to establish standards for device-device authentication such that interoperability is not impeded.
Action Item 2.4.2	In situations where the provider is accessing an EHR or Health Information Exchange external to the hospital or clinical environment, the health care

Imperative 2	Increase the security and resilience of medical devices and health IT.
	industry should adopt the NIST SP 800-46 guidelines for remote access including the use of two-factor authentication to ensure a compromised password cannot alone be used to gain access.
Recommendation 2.5	**Employ strategic and architectural approaches to reduce the attack surface for medical devices, EHRs, and the interfaces between these products.**
Action Item 2.5.1	Manufacturers should focus on architecturally supporting security interoperability for their products that validate, and leverage health care delivery organizations existing security controls.
Action Item 2.5.2	Industry should establish a task force to collaborate on issues related to risks and challenges of product interdependencies and two-way data flows. These interdependencies include medical devices, EHRs, Internet of Things (IoT), and two-way data flows.
Action Item 2.5.3	HHS should evaluate existing authorities and identify gaps to conduct cybersecurity surveillance of medical devices and EHRs.
Action Item 2.5.4	Industry should build and anticipate the need for IT forensics to accompany adverse event investigations by ensuring that logs exist and are accessible.
Action Item 2.5.5	Health care providers should ensure collaboration among department leadership, biomedical engineering teams, IT staff, and IT security in the selection, deployment, and maintenance of medical devices.
Recommendation 2.6	**Establish a Medical Computer Emergency Readiness Team (MedCERT) to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures.**
Action Item 2.6.1	Federal agencies must partner with industry to define the scope and scale of a MedCERT. The MedCERT would be a trusted entity that is viewed as independent and neutral by all stakeholders and will work to arrive at “the ground truth” of vulnerabilities and proposed mitigations.
Action Item 2.6.2	In order to validate the vulnerabilities and impacts, as well as assess the public fixes (mitigations and patches), the MedCERT will need to rely upon the technical analyses provided by independent certification and testing capabilities. These technical analyses provided by individual testing labs will need to be correlated to support the MedCERT’s vulnerability validation and assessment roles.

Imperative 3	Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
Recommendation 3.1	**Every organization must identify the cybersecurity leadership role for driving for more robust cybersecurity policies, processes, and functions with clear engagement from executives.**
Action Item 3.1.1	Industry should establish best practices for the qualifications and governance models that support the cybersecurity and privacy leadership role within their organizations.
Action Item 3.1.2	Industry should establish governance structures to empower Chief Information Security Officers (CISO) to express risks and advocate for resources with organizational leadership.
Action Item 3.1.3	Industry should identify opportunities for defining shared or third party CISO roles for small organizations.
Recommendation 3.2	**Establish a model for adequately resourcing the cybersecurity workforce with qualified individuals.**
Action Item 3.2.1	Industry should develop a research report, similar to the California Safe Patient Ratio, to identify appropriate voluntary benchmarks for cybersecurity staffing per patient accounting for various exceptions/factors (e.g., research centers/academic medical centers/ambulatory versus inpatient facilities).
Action Item 3.2.2	HHS should consider options, in coordination with industry partners, to develop a conformity assessment program to establish standards for different roles within the health care industry and authorize education providers against those standards.
Action Item 3.2.3	Organizations such as the Committee on National Security Systems (CNSS), the National Centers of Academic Excellence in Cyber Defense (CAE-CD), DHS, or NIST should consider establishing mechanisms to assist in developing the requirements for and certifying advanced degree cybersecurity programs.
Action Item 3.2.4	Industry should define mechanisms to educate and better leverage clinicians, in a tiered workforce model, capable of fundamental cybersecurity-related tasks.
Action Item 3.2.5	Congress should provide financial support to CNSS and CAE-CD for cybersecurity education certification to ensure core competencies for health care cybersecurity professionals.
Action Item 3.2.6	Industry and the federal government should explore opportunities for individuals to engage in ongoing internship programs to develop more information security professionals in supporting the health care industry.
Recommendation 3.3	**Create managed security service provider (MSSP) models to support small and medium-size health care providers.**
Action Item 3.3.1	The federal government should evaluate incentive options, such as grants and tax incentives, to encourage more MSSPs to achieve economies of scale to support small and medium-size health care providers.
Action Item 3.3.2	Federal regulatory agencies should evaluate incentive options, such as crediting small and medium-size health care providers who have engaged

Imperative 3	Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
	MSSPs during their audits and breach investigations, to encourage providers to leverage MSSPs.
Action Item 3.3.3	Industry and the federal government should explore opportunities for individuals to engage in ongoing internship programs (e.g., at MSSPs and federal agencies) to develop more information security professionals in supporting the health care industry.
Recommendation 3.4	**Small and medium sized health care providers should evaluate options to migrate patient records and legacy systems to secure environments (e.g., hosted, cloud, shared computer environments).**
Action Item 3.4.1	The federal government should evaluate incentive options, such as grants, to encourage industry to develop secure options for supporting small and medium-size health care organizations.
Action Item 3.4.2	The federal government should evaluate incentive options, such as tax incentives, to encourage health care providers migrate to more secure environments including hosted services (i.e., vendors or other providers) or cloud service providers.
Action Item 3.4.3	Federal regulatory agencies should provide additional guidance to service providers (including HHS-compliant Business Associate Agreements) that wish to align their security management practices with the *Health Insurance Portability and Accountability Act* (HIPAA) and create increased awareness among health care providers that alternative technologies exist to store, access, share, and process their data.
Action Item 3.4.4	Industry should develop use cases and contracts tailored for these small and medium-size organizations.
Action Item 3.4.5	Insurance companies should provide more incentives to encourage small and medium-size health care service providers who migrate to a more secure environment than the one in which they currently operate.

Imperative 4	Increase health care industry readiness through improved cybersecurity awareness and education.
Recommendation 4.1	**Develop executive education programs targeting Executives and Boards of Directors about the importance of cybersecurity education.**
Action Item 4.1.1	Trade and professional associations should ensure cyber workforce training and education focuses on corporate officers and Boards of Directors communication.
Action Item 4.1.2	Trade and professional associations in the health care industry should develop materials for CISOs and security leaders to better communicate with executive level leadership and Boards of Directors regarding security risks, priorities, and cyber hygiene posture.

Imperative 4	Increase health care industry readiness through improved cybersecurity awareness and education.
Action Item 4.1.3	Health care organizations should participate in National Cybersecurity Awareness Month events in their area and become partners of the National Cybersecurity Awareness Campaign, managed through DHS as a baseline to build and customize for the HPH Sector.
Recommendation 4.2	**Establish a cybersecurity hygiene posture within the health care industry to ensure existing and new products/systems risks are managed in a secure and sustainable fashion.**
Action Item 4.2.1	Industry should manage all health care infrastructure technology (including IoT) security to focus on patient safety, both on an individual and population basis, with an appreciation of how the technology will be used and how it could be misused.
Action Item 4.2.2	Industry should ensure that no known malware exists in newly produced equipment/software entering the market (i.e., premarket), and there should be ongoing surveillance for malware in equipment/software currently in the market (i.e., postmarket).
Action Item 4.2.3	Health care organizations must develop a strategy for cybersecurity hygiene for existing and legacy equipment, a systematic approach for patching, implementation of compensating controls, isolation, and/or replacement (as available or applicable) should be applied. For newly produced equipment/software entering the market, device manufacturers should have a plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device.
Recommendation 4.3	**Establish a conformity assessment model for evaluating cybersecurity hygiene that regulatory agencies and industry could rely on, instead of a diversity of auditors.**
Action Item 4.3.1	Health care regulatory agencies in partnership with industry should establish the requirements for a common set of requirements upon which the conformity assessment program would be built.
Action Item 4.3.2	The federal government should resource and establish a process for the oversight of the conformity assessment program.
Action Item 4.3.3	Health care regulatory agencies should develop strategies to begin to phase in certifiers who have been accredited under the conformity assessment program.
Action Item 4.3.4	The federal government in coordination with industry should develop a business model/incentives to ensure that the testing, validation, and certification data is widely available to health care providers, regardless of size and resources.
Action Item 4.3.5	Health care regulatory agencies should be familiar and continue to build upon the National Cybersecurity Workforce Framework for an understanding of cybersecurity roles, responsibilities, and the knowledge, skills, and abilities required for each cybersecurity role. The Workforce Framework is available at Workforce Framework.

Imperative 4	Increase health care industry readiness through improved cybersecurity awareness and education.
Recommendation 4.4	**The NIST Baldrige Cybersecurity Excellence Builder, should be further developed: 1) specific to health care, and 2) specific to the types of health care operations that are widely deployed across the industry and have limited access to cybersecurity resources (e.g., small hospitals or practices, rural locations with limited access to security resources).**
Action Item 4.4.1	HHS and NIST should develop a health care specific version of this tool.
Action Item 4.4.2	HHS and NIST should develop a tiered version of the tool for the industry based on size and business model (e.g., physician practice, clinic, hospital, Academic Medical Center, business associates).
Action Item 4.4.3	In order to establish an industry-wide baseline, the self-assessment should be required for all Covered Entities while granting exemption or partial exemption to fines or prosecution as a result of that assessment and corrective action plans.
Recommendation 4.5	**Increase outreach and engagement for cybersecurity across federal, state, local, tribal, territorial, and the private sector partners through an education campaign including meetings, conferences, workshops, and tabletop exercises across regions and industry.**
Action Item 4.5.1	HHS should work with government and industry partners to develop an outreach and engagement campaign to increase health care cybersecurity awareness and literacy among health care providers, patients, and IT professionals.
Action Item 4.5.2	HHS should work with government and industry partners to develop a specific outreach program for health care executives, so that they can have a better understanding of the importance of cybersecurity in their own organizations and can better engage with cybersecurity professionals to ensure that protective programs are adequately managed and resourced.
Action Item 4.5.3	HHS should work with government and industry partners to develop a series of workshops to explore current questions in health care cybersecurity, such as evaluation of best practices, research and development (R&D) needs, and the role of insurance.
Action Item 4.5.4	HHS should work with government and industry partners to develop educational materials for patients to assist them in accessing, managing, and protecting their health care information.
Action Item 4.5.5	HHS should work with government and industry partners to develop a national health care cyber-literacy course that is updated on a biannual basis to keep up with rapidly changing technology and to train health care professionals on the importance of cybersecurity in their day-to-day tasks. Industry at all levels should incorporate principles from this course into all patient education modules or courses, as applicable.

Imperative 4	Increase health care industry readiness through improved cybersecurity awareness and education.
Action Item 4.5.6	HHS should work with government and industry partners to develop a health care mentoring program to help educate non-IT staff to proper risk management of IT and information sharing.
Action Item 4.5.7	HHS should identify privacy experts, patient advocates, regulatory experts, and proprietary information experts to discuss issues related to fraud or stock manipulation.
Recommendation 4.6	**Provide patients with information on how to manage their health care data, including a cybersecurity and privacy grading system for consumers to make educated decisions when selecting services or products around non-regulated health care services and products.**
Action Item 4.6.1	The Federal Trade Commission (FTC) should engage health care and consumer organizations to develop a process to evaluate, assess, and rate health care/lifestyle products. This aligns to action item 3.1.3 of the Commission on Enhancing National Cybersecurity's Report on Securing and Growing the Digital Economy.
Action Item 4.6.2	HHS, DHS, NIST, and FTC should establish a grant or national challenge for a consumer grading system.

Imperative 5	Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
Recommendation 5.1	**Develop guidance for industry and academia on creating economic impact analysis and loss for cybersecurity risk for health care research and development.**
Action Item 5.1.1	The federal government should work with industry to establish a task force to develop risk models for evaluating U.S. economic and organizational impact for cybersecurity failures.
Action Item 5.1.2	Industry should develop best practices to balance academic freedom, intellectual property, and health care services.
Action Item 5.1.3	HHS should partner with the DHS Science and Technology Directorate to identify grand challenges, priorities, and implement new research to support small and rural organizations.
Action Item 5.1.4	Congress should identify resources for improving research addressing small and rural provider security challenges.
Action Item 5.1.5	HHS should partner with DHS and Office of the Director of National Intelligence to identify specific threat actors and the techniques that they employ to target U.S. health care R&D information. This information should be updated regularly to stay abreast of emerging tactics and techniques.
Action Item 5.1.6	HHS should present findings from Action Item 5.1.5 to senior executives and other representatives from the R&D industry.

Imperative 5	Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
Recommendation 5.2	**Pursue research into protecting health care big data sets.**
Action Item 5.2.1	Entities that manage big data solutions should ensure that a detailed risk assessment is performed at frequent intervals and that they address 100 percent of preventative security controls, including continuous monitoring programs to mitigate inappropriate access.
Action Item 5.2.2	Entities that manage big data solutions should have detailed documentation of source and destination connections and diligent review and approval process in managing these connections.
Action Item 5.2.3	Entities that manage big data solutions should apply minimum necessary security principles in providing users/organizations with access to these systems to mitigate disastrous situations with these systems.
Action Item 5.2.4	Health care providers should exercise solid due diligence processes when selecting third party solutions or cloud based solutions, as well as ensure that sufficient administrative safeguards are in place, including an unlimited indemnification clause in case of data breaches.
Action Item 5.2.5	Entities that manage big data solutions should apply extreme care in determining what data is collected, what data is retained, and what data is deleted as more data presents increased security risks.

Imperative 6	Improve information sharing of industry threats, risks, and mitigations.
Recommendation 6.1	**Tailor information sharing for easier consumption by small and medium-size organizations who rely on limited or part-time security staff.**
Action Item 6.1.1	HHS in cooperation with the Information Sharing and Analysis Organizations (ISAO) should streamline and consolidate information sharing data on threats whenever practical for easier consumer adoption.
Action Item 6.1.2	Industry should incentivize the adoption of information sharing for small and medium-sized organizations for MSSPs.
Recommendation 6.2	**Broaden the scope and depth of information sharing across the health care industry and create more effective mechanisms for disseminating and utilizing data.**
Action Item 6.2.1	HHS in coordination with ISAOs should evaluate incorporating hazards (e.g., national disasters, acts of terrorism, pandemic outbreaks) with the potential to disrupt critical health infrastructure in their information sharing threat analysis.
Action Item 6.2.2	HHS should work with all federal partners to ensure that intelligence reports and threat information is consolidated and given additional context as distributed to industry.
Action Item 6.2.3	HHS should partner with industry to identify health care subsector priorities for intelligence reporting. For example, payers may be extremely interested in

Imperative 6	Improve information sharing of industry threats, risks, and mitigations.
	information regarding medical insurance fraud and emerging cybercrime tactics that are used to support this activity, whereas pharmaceutical companies are likely to be very interested in the changing methods used by nation state actors to steal intellectual property.
Action Item 6.2.4	HHS and the ISAO should continue to work with DHS and other entities to develop processes for quickly curating and releasing critical threat information.
Recommendation 6.3	**Encourage annual readiness exercises by the health care industry.**
Action Item 6.3.1	HHS and industry should identify those critical incident response plans that could be best leveraged by the health care industry.
Action Item 6.3.2	Industry should implement cybersecurity incident response plans, which are reviewed and tested annually.
Action Item 6.3.3	HHS, DHS National Cybersecurity and Communications Integration Center, and law enforcement should maintain unified and dedicated channels during steady state and response efforts to: 1) provide subject matter expertise to issues that involve the HPH Sector; 2) leverage existing sector relationships across government, within industry, and with an impacted entity; and 3) facilitate targeted dissemination, clarification, and near real-time notifications to the health care industry in a strategically sequenced manner.
Recommendation 6.4	**Provide security clearances for members of the health care community.**
Action Item 6.4.1	HHS, DHS, and the FBI should review the HPH Sector's utilization of the Private Sector Clearance Program to identify gaps and strengthen the criteria and process through which health care industry partners can apply for clearances.

Appendix B: Task Force Meeting Agendas and Speakers

This appendix lists all public and private session HCIC Task Force meetings, agenda topics, and associated speakers. Briefings covered a wide range of topics to assist the Task Force in addressing its charge under the Act and to develop this report and associated recommendations.

Table 2 Task Force Meeting Dates

Date	Location
March 16, 2016	Task Force Teleconference
April 21, 2016	United States Access Board –Washington, DC
May 19, 2016	Task Force Teleconference
June 16, 2016	Task Force Teleconference
July 21, 2016	Deloitte – Arlington, VA
August 18, 2016	Task Force Teleconference
September 15, 2016	Task Force Teleconference
October 26-27, 2016	HHS – Washington, DC
November 17, 2016	Task Force Teleconference
December 14-15, 2016	DHS – Arlington, VA and Deloitte – Arlington, VA
January 12, 2017	Task Force Teleconference
January 19, 2017	Task Force Teleconference
February 9, 2017	Task Force Teleconference
February 20, 2017	Teleconference and Healthcare Information and Management Systems Society (HIMSS) Conference – Orlando, FL
March 9, 2017	Task Force Teleconference
March 16, 2017	Task Force Teleconference

Table 3 March 16, 2016 Agenda

Wednesday, March 16, 2016 – Task Force Teleconference
Welcome and Introductions • Kathryn Martin – Counselor to the Secretary for Health Policy, HHS
Introduction of HCIC Task Force Members • Steve Curren – Director, Division of Resilience, ASPR, HHS
The Act Overview • Emery Csulak – CISO, CMS and Task Force Co-Chair
HCIC Task Force Member Selection Process

Wednesday, March 16, 2016 – Task Force Teleconference
• Emery Csulak – CISO, CMS and Task Force Co-Chair
HCIC Task Force Structure, Operations, and Requirements • Emery Csulak – CISO, CMS and Task Force Co-Chair
Meeting Cadence and Logistical Items • Emery Csulak – CISO, CMS and Task Force Co-Chair

Table 4 April 21, 2016 Agenda

Thursday, April 21, 2016 – United States Access Board, Washington, DC
Public Session: Welcome and Introductions • Mary K. Wakefield, PhD – Acting Deputy Secretary, HHS
Public Session: Health Care Industry Cybersecurity Task Force Overview • Emery Csulak – CISO, CMS and Task Force Co-Chair • Theresa Meadows – Senior Vice President and Chief Information Officer, Cook Children's Health Care System and Task Force Co-Chair
Public Session: DHS/NIST Cross-Sector Overview • Laura Laybourn – Director, Stakeholder Engagement and Cyber Infrastructure Resilience, Office of Cybersecurity and Communications, DHS • Matthew Barrett – Program Manager, Cybersecurity Framework, NIST
Public Session: Cybersecurity Best Practices – Energy Sector Panel • Mike Smith – Senior Cyber Policy Advisor, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy • Fowad Muneer – Program Manager, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy • Nadya Bartol – Vice President, Industry Affairs and Security Strategist, Utilities Telecom Council
Public Session: Cybersecurity Best Practices – Banking and Finance Sector Panel • Brian Peretti – Director, Office of Critical Infrastructure Protection and Compliance Policy, U.S. Department of the Treasury • John Carlson – Chief of Staff, Financial Services Information Sharing and Analysis Center
Discussion of Potential Task Force Activities and Products
Discussion of Media Engagement

Table 5 May 19, 2016 Agenda

Thursday, May 19, 2016 – Task Force Teleconference
Cybersecurity Best Practices – Banking and Finance Sector • Jenny Menna – Vice President, Cybersecurity Partnership Executive, U.S. Bank
Discussion of Potential Task Force Activities and Products

Table 6 June 16, 2016 Agenda

Thursday, June 16, 2016 – Task Force Teleconference
Discussion of Product Deliverables
Discussion of Framework
Proposal of Workstream Breakouts

Table 7 July 21, 2016 Agenda

Thursday, July 21, 2016 – Deloitte, Arlington, VA
Task Force Table Talks
Preliminary Observations and Recommendations Discussion
Public Session: Cybersecurity Best Practices – Finance and Health Care Information Sharing and Analysis Center Sector Panel • Jim Routh – Chief Security Officer, Vice President, Aetna Inc.
Public Session: Discussion of Medical Device Workshop – 2 Day Workshop Out Brief • Aftin Ross, PhD – Senior Project Manager, FDA
Public Session: Task Force Progress Out Brief
CYBERSTORM V National Cybersecurity Exercise Presentation • Gabriel Taran – Assistant General Counsel for Cyber and Infrastructure Programs, DHS • Timothy McCabe – National Cyber Exercise and Planning Program (NCEPP) Lead, DHS • Dawn Page – NCEPP/Healthcare Public Health Community Lead for Cyber Storm V, DHS
Discussion of Medical Device Cybersecurity Ecosystem • Margie Zuk – Senior Principal Cybersecurity Engineer, MITRE Corporation

Table 8 August 18, 2016 Agenda

Thursday, August 18, 2016 – Task Force Teleconference
Task Force Workstream Out-Briefs
Review Risk Framework and Discussions
Discuss Education and Information Sharing Objectives

Table 9 September 15, 2016 Agenda

Thursday, September 15, 2016 – Task Force Teleconference
Task Force Workstream Out-Briefs
Review Report Examples and Draft Report Outline

Table 10 October 26-27, 2016 Agendas

Wednesday, October 26, 2016 – HHS, Humphrey Building, Washington, DC Thursday, October 27, 2016 – HHS, O'Neill , Washington, DC
Public Session: Opening Remarks • Emery Csulak – CISO, CMS and Task Force Co-Chair
Public Session: Panel Discussion – The Federal Approach for Health Care Industry Cybersecurity • Leo Scanlon – Acting CISO, HHS • Iliana Peters – Senior Advisor for HIPAA Compliance and Enforcement, OCR, HHS • Lucia Savage – Chief Privacy Officer, ONC, HHS • Steve Curren – Director, Division of Resilience, ASPR, HHS • Suzanne Schwartz, MD – Center for Devices and Radiological Health (CDRH) Associate Director for Science and Strategic Partnerships, FDA • Theresa Meadows (Moderator) – Senior Vice President and Chief Information Officer, Cook Children's Health Care System and Task Force Co-Chair
Public Session: Panel Discussion – Commercial Sector Information Sharing • Matt Hartley – Vice President Intel Operations & Products, FireEye • Anna Turman – Chief Information Officer, Chadron Community Hospital • Angela Diop – Vice President Information Systems, Unity Health Care • Matthew Snyder – CISO, Penn State Hershey Medical Center and Health System • Daniel Nutkis – Founder and Chief Executive Officer, Health Information Trust Alliance

Wednesday, October 26, 2016 – HHS, Humphrey Building, Washington, DC Thursday, October 27, 2016 – HHS, O'Neill , Washington, DC
• Terry Rice – National Health Information Sharing and Analysis Center (NH-ISAC), Board of Directors Member, and Vice President IT Risk Management and CISO, Merck & Co. • Emery Csulak (Moderator) – CISO, CMS and Task Force Co-Chair
Extended Q&A with Panelists
Information Sharing Challenges for Small Organizations • Daniel Nutkis – Founder and Chief Executive Officer, Health Information Trust Alliance
College of Healthcare Information Management Executives (CHIME) Survey Results Discussion • Mari Savickis – Vice President, Federal Affairs, CHIME
Task Force Workstream Out-Briefs and Working Session
Task Force Next Steps and Developing the Report to Congress

Table 11 November 17, 2016 Agenda

Thursday, November 17, 2016 – Task Force Teleconference
Task Force Workstream Out-Briefs
Round Robin: Top 3 Concerns for the Health Care Industry
Health Care Industry Specific Break-Out Discussion
Report and Recommendations Development Working Session

Table 12 December 14-15, 2016 Agendas

Wednesday, December 14, 2016 – DHS, Arlington, VA Thursday, December 15, 2016 – Deloitte, Arlington, VA
Opening Remarks
Report and Recommendations Development Working Session
Discussion: Commission on Enhancing National Cybersecurity Report • Kevin Stine – Chief, Applied Cybersecurity Division Information Technology Laboratory, NIST
Dependencies in the HPH Sector • Alex Reniers – Office of Cyber and Infrastructure Analysis, DHS • Titus Bickel – Office of Intelligence and Analysis, DHS
Report and Recommendations Development Working Session
HIMSS EHR Association Discussion • Justin Armstrong – MEDITECH, Privacy and Security Workgroup

Wednesday, December 14, 2016 – DHS, Arlington, VA **Thursday, December 15, 2016 – Deloitte, Arlington, VA**
• Ross Berning – Epic, Privacy and Security Workgroup • Ann Marie Dunn – MEDITECH, Privacy and Security Workgroup • Isis Esteves – MEDITECH, Privacy and Security Workgroup • Eli Fleet – Director, Federal Affairs, HIMSS • Sarah Willis Garcia – Program Manager, EHRA, HIMSS • Barbara Hobbs – MEDITECH, Privacy and Security Workgroup • Michael Hunt – Evident, Privacy and Security Workgroup • Lee Kim – Director, Privacy and Security, HIMSS • Dan Levene – Cerner, Privacy and Security Workgroup • Nam Nguyen – Practice Fusion (Chair, Privacy and Security Workgroup) • Nancy Ramirez – Senior Associate, EHRA, HIMSS • Suzanne Smeltzer – Greenway, Privacy and Security Workgroup • Sam Snider – Greenway, Privacy and Security Workgroup • Peter Wallace – Varian, Privacy and Security Workgroup
Medical Device Guidance vs Regulation • Suzanne Schwartz, MD – CDRH Associate Director for Science and Strategic Partnerships, FDA
Report and Recommendations Development Working Session
Educational Resources for the Health Care Industry • Margie Zuk – Senior Principal Engineer, MITRE • Penny Chase – Senior Principal Scientist, MITRE
Public Session: America's Health Insurance Plans (AHIP) Presentation • Marilyn Zigmund Luke – Vice President, Special Projects, Executive Office, AHIP
Public Session: HIMSS Presentation • Jeff Coughlin – Senior Director, Federal and State Affairs, HIMSS
Public Session: Medical Device Innovation, Safety and Security Consortium Discussion • Dale Nordenberg, MD – Chief Executive Officer, Novasano Health and Science

Table 13 January 12, 2017 Agenda

Thursday, January 12, 2017 – Task Force Teleconference
DHS Cybersecurity R&D Initiatives Discussion • Dan Massey, PhD – Program Manager, Cyber Security Division for the Homeland Security Advanced Research Projects Agency, DHS
HIMSS Cybersecurity Data Discussion • Lee Kim, JD – Director, Privacy and Security, HIMSS
Information Sharing Activities and Task Force Recommendations Discussion • Denise Anderson – President, NH-ISAC
Microsoft Products: Health Care Industry Approach and Considerations • Hector Rodriguez – Director, U.S. Health & Life Sciences Industry Specialist Team, Microsoft

Table 14 January 17, 2017 Agenda

Thursday, January 17, 2017 – Task Force Teleconference
Review Draft Task Force Report

Table 15 February 9, 2017 Agenda

Thursday, February 9, 2017 – Task Force Teleconference
Informational Briefing: Anti-Kickback Statute & The Physician Self-Referral Law • Lisa Wilson – Senior Technical Advisor, CMS • Heather Westphal – Senior Counsel, Industry Guidance Branch, Office of Counsel to the Inspector General, HHS • Matthew Edgar – Health Insurance Specialist, CMS
Review Draft Task Force Report

Table 16 February 20, 2017 Agenda

Monday, February 20, 2017 – Teleconference and HIMSS Conference – Orlando, FL
Review and Refine Draft Recommendations and Report
Overview of HHS Office of the Chief Information Officer Organizational Relationships • Chris Wlaschin – CISO, HHS • Beth Killoran – Chief Information Officer, HHS • Leo Scanlon – Deputy CISO, HHS • Matthew Olsen – Acting Chief Privacy and Data Sharing Officer, HHS

Table 17 March 9, 2017 Agenda

Thursday, March 9, 2017 – Task Force Teleconference
Review and Refine Draft Recommendations and Report

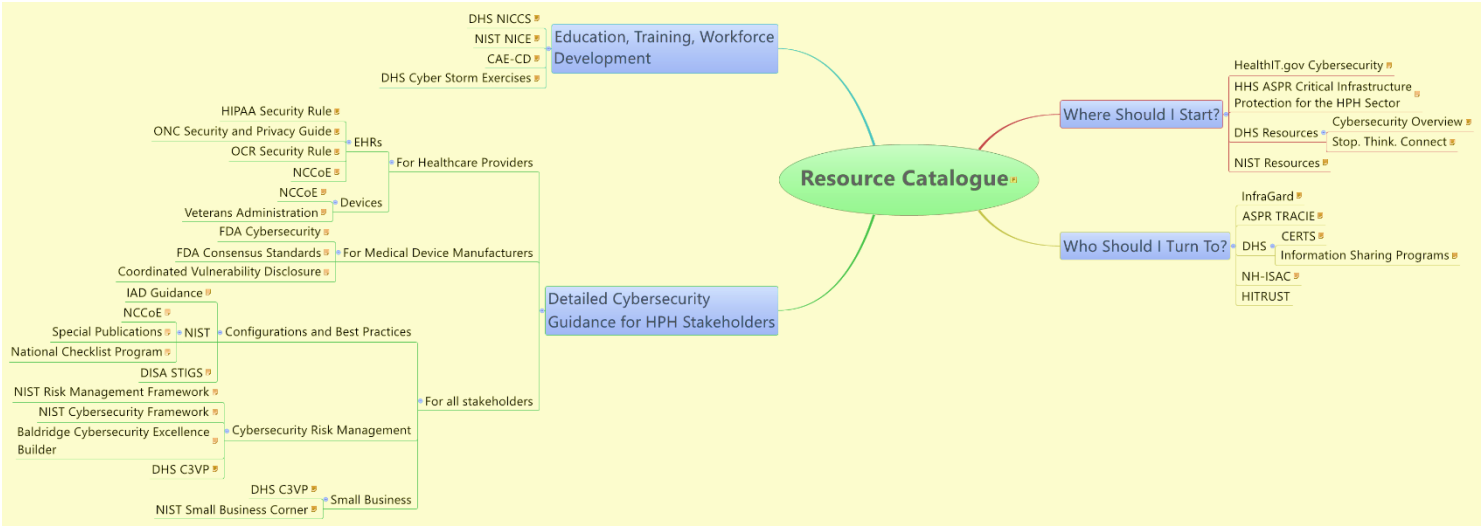
Table 18 March 16, 2017 Agenda

Thursday, March 16, 2017 – Task Force Teleconference
Review and Approve the HCIC Report

Appendix C: Resource Catalog

Pursuant to the task identified in the Act, this appendix summarizes a number of the key resources available to the sector. The Task Force made every effort to be comprehensive, while identifying resources that are easily accessible and publically available. The mind map in Figure 5 below visually depicts the connection of resources contained in the appendix.

Figure 5 Resource Mind Map



1. Where Should I Start?

HHS Resources

HealthIT.gov Cybersecurity: HHS ONC has developed resources for health care cybersecurity and risk management. The HealthIT.gov Cybersecurity website points to these resources, including the Top Ten Tips and cybersecurity training games.

HealthIT Cybersecurity Shared Responsibility

HHS Office of the Assistant Secretary for Preparedness and Response (ASPR): ASPR's Technical Resources, Assistance Center, and Information Exchange (TRACIE) was created to meet the information and technical assistance needs of regional ASPR staff, health care coalitions, health care entities, health care providers, emergency managers, public health practitioners, and others working in disaster medicine, health care system preparedness, and public health emergency preparedness.

The resources in the Cybersecurity Topic Collection can help stakeholders better protect against, mitigate, respond to, and recover from cyber threats, to ensure patient safety and operational continuity.

ASPR TRACIE Cybersecurity

DHS Resources

Cybersecurity Overview: Strengthening the security and resilience of cyberspace is an important part of DHS's mission. This website points to the many resources and programs DHS makes available.

DHS Cybersecurity Overview

Stop. Think. Connect: DHS's "Stop. Think. Connect." Campaign is aimed at increasing the understanding of cyber threats and empowering the public to be more secure online. The toolkit provides resources for all segments of the public.

DHS StopThinkConnect

NIST Resources

NIST develops cybersecurity standards and best practices that address interoperability, usability, and privacy. The NIST Cybersecurity website provides an overview of their programs (including the National Cybersecurity Center of Excellence and the Cybersecurity Framework) and pointers to specific cybersecurity topics.

NIST Cybersecurity

2. Who Should I Turn To?

Healthcare and Public Health (HPH) Sector Critical Infrastructure Protection Partnership: HHS/ASPR's Critical Infrastructure Protection Program leads a public and private sector partnership to protect the HPH Sector from all hazards, including cyber threats. Health care industry organizations can join the partnership's HPH Sector Coordinating Council (HSCC). The HSCC is an independent, industry-led group that works closely with HHS and other governmental partners to address cybersecurity and other critical infrastructure issues through a collaborative partnership approach.

HHS ASPR Critical Infrastructure Protection

HITRUST*:* The HITRUST Alliance is a not for profit organization that collaborates with public and private sector leaders from health care technology, privacy, and information security organizations. HITRUST's focus is to promote the protection of health information and manage the risk to that information. HITRUST provides a range of frameworks, related assessment and assurance methodologies, and programs that support cyber sharing, analysis, and resilience.

HITRUST

National Health – Information Sharing and Analysis Center (NH-ISAC)

NH-ISAC: The NH-ISAC is the official ISAC for the HPH sector. It is a membership organization that enables sharing cybersecurity threat information, best practices, and mitigations across the sector.

NH ISAC

InfraGard: InfraGard is a partnership between the FBI and the private sector dedicated to sharing information and intelligence to counter threats.

InfraGard

DHS

U.S. Computer Emergency Readiness Team (US-CERT): The US-CERT develops actionable information to the public and private sectors. The National Cyber Awareness System publishes alerts about current cybersecurity issues, weekly vulnerability bulletins, advice and best practices, and in-depth technical articles.

US CERT

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): The ICS-CERT coordinates among federal, state, local, and tribal governments and the private sector about cybersecurity vulnerabilities, incidents, and mitigations related to industrial control systems, include medical devices.

ICS CERT

Information Sharing Programs: This is the landing page for DHS' various programs for sharing cybersecurity information with private industry, including Automated Indicator Sharing, Cyber Information Sharing and Collaboration Program, Enhanced Cybersecurity Services, ISAOs, and the National Cybersecurity and Communications Integration Center.

DHS NCCIC

3. Detailed Cybersecurity Guidance for HPH Stakeholders

For Health Care Providers – EHRs

HIPAA Security Rule: OCR provides a summary of the HIPAA Security Rule.

HIPAA Security Rule

ONC Security and Privacy Guide: ONC, in coordination with OCR, created a guide to privacy and security of electronic health information, along with a Security Risk Assessment Tool.

ONC Security and Privacy Guide

OCR Security Rule: OCR created a collection of resources on the HIPAA Security Rule, including guidance for implementing the security standards, risk analysis, pointers to key NIST documents, and OCR Awareness Newsletters on vulnerabilities and threats.

OCR Security Rule

National Cybersecurity Center of Excellence (NCCoE): One of the NCCoE health IT projects is related to EHRs on mobile devices.

NCCoE EHRs on Mobile Devices

For Health Care Providers – Devices

NCCoE: One of the NCCoE health IT projects is related to wireless infusion pumps.

NIST NCCoE Wireless Infusion Pumps

Veterans Affairs: Veterans Affairs Directive 6550 establishes the technical assessment requirements for pre-procurement of medical devices/systems, including those that are connected to Veterans Affairs systems or contain patient sensitive information. The appendix is a questionnaire that health care providers can use to evaluate the configuration and security profile of medical devices during acquisition planning to identify potential risks and integrate devices into hospital operations. The 6550 questionnaire extends the Manufacturer Disclosure Statement for Medical Device Security, which was developed by HIMSS and the American College of Clinical Engineering, and then standardized through a joint effort between HIMSS and the National Electrical Manufacturers Association.

VA Directive 6550

For Medical Device Manufacturers

FDA Cybersecurity: FDA's Cybersecurity web page summarizes FDA's activities related to medical device cybersecurity, including issuing premarket and postmarket guidance, issuing Safety Communications for vulnerabilities discovered in devices, convening public workshops, and entering into a Memorandum of Understanding with the NH-ISAC and the Medical Device Innovation, Safety and Security Consortium.

FDA Cybersecurity

FDA Consensus Standards: FDA recognizes several consensus standards related to medical device security. Quick search for "security" in the database.

FDA Consensus Standards

Coordinated Vulnerability Disclosure: An important element of FDA's postmarket guidance is developing coordinated disclosure policies for medical device vulnerabilities. ISO/IEC 29147 - Information technology - Security techniques - Vulnerabilities provides guidelines for vendors to include in their business processes when receiving information about potential vulnerabilities and distributing vulnerability resolution information.

ISO Coordinated Vulnerability Disclosure Standards

For all stakeholders – Configurations and Best Practices

IAD Guidance: Information assurance at the National Security Agency provides security solution guidance based upon their unique and deep understanding of risks, vulnerabilities, mitigations, and threats. This information can be utilized to harden and defend network and system infrastructure, while providing for a sustained presence. This guidance covers a broad range of topics including secure architectures, configuration guidance for networks and industrial control systems, and security tips.

IAD Guidance

NIST NCCoE: The NIST NCCoE accelerates the private sector's adoption of advanced, standards-based security technologies by developing use cases, working with vendors to develop solutions in NCCoE's labs, and publish practice guides (in NIST Special Publication 1800 series).

NIST NCCoE

NIST Special Publications: The NIST Special Publications 800 series provides computer/cyber/information security guidelines, recommendations, and reference materials. Special Publication 800-53 provides a catalog of security and privacy controls for use in federal information systems, which many private enterprises find useful for establishing their security controls. There are a wide range of guides to help securely implement various technologies (e.g., servers, mobile devices, cloud computing, encryption, and wireless protocols).

The NIST Special Publication 1800 series consists of practical guides that provide standards based approaches to cybersecurity challenges in the public and private sectors.

NIST Special Publications

NIST National Checklist Program: The National Checklist Program is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low-level guidance on setting the security configuration of operating systems and applications.

NIST National Checklist Program

Defense Information Systems Agency (DISA) publishes the Security Technical Implementation Guides (STIGs): DISA publishes the STIGs, which provide configuration guidance for information assurance enabled Department of Defense systems. Even though these STIGS provide configurations for Department of Defense systems, manufacturers and health care providers can adopt configurations for their systems (medical devices and health IT systems) and networks.

Some relevant STIGS are Application Security and Development STIG, Multifunction Device and Network Printers STIG, and Network Device Management STIG.

DISA Security Technical Implementation Guides

For all stakeholders – Cybersecurity Risk Management

NIST Risk Management Framework: The NIST Risk Management Framework provides an effective framework for selecting the appropriate security controls for a system—the security controls necessary to protect individuals and the operations and assets of the organization—by managing organizational risk. The Risk Management Framework provides a process that integrates security and risk management activities into the system development lifecycle. The risk management concepts are intentionally broad-based with the specific details of assessing

risk and employing appropriate risk mitigation strategies provided by the supporting NIST security standards and guidelines.

NIST Cybersecurity Risk Management Framework

NIST Cybersecurity Framework: The NIST Cybersecurity Framework website contains the latest version of the Framework, a reference tool (a database implementing the framework core), and industry resources.

NIST Cybersecurity Framework

Baldrige Cybersecurity Excellence Builder: NIST's Baldrige Cybersecurity Excellence Builder is a voluntary self-assessment tool that enables organizations to better understand the effectiveness of their cybersecurity risk management efforts. It blends the systems perspective and business practices of the Baldrige Excellence Framework with the concepts of the NIST Cybersecurity Framework.

Baldrige Cybersecurity Excellence Builder

DHS Critical Infrastructure Cyber Community C³ Voluntary Program (C3VP): The C3VP aims to support industry efforts to increase cyber resilience, awareness and use of the NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity and encourage organizations to manage cybersecurity as part of an all-hazard approach to enterprise risk management.

The C3VP website contains information about the Cybersecurity Framework, including sector-specific guidance, and resources for business organized by the framework. In addition, the Assessments section of the C3VP website contains information on the Cyber Resiliency Review program, a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices, which can be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.

DHS C3VP

For all stakeholders – Small Business

DHS C3VP: DHS C3VP has resources to help small and medium businesses address their cybersecurity risks, given the scope and complexity of the issue in the face of a small staff and limited resources.

DHS C3VP Small Business

NIST Small Business Corner: NIST's Small Business Corner website has cybersecurity resources for small businesses. NIST, the FBI, and the Small Business Administration conduct workshops on cybersecurity threats and solutions. The Small Business Corner Library contains

workshop materials and a link to NIST Internal/Interagency Report 7621 r1: *Small Business Information Security: The Fundamentals*.

NIST Small Business Corner

4. Education, Training, Workforce Development

DHS National Initiative for Cybersecurity Careers and Studies (NICCS): DHS's NICCS provides a collection of resources on cybersecurity education, including a catalogue of courses, information about the National Centers of Academic Excellence program managed by National Security Agency, K-12 resources, and industry resources.

DHS NICCS

NIST National Initiative for Cybersecurity Education (NICE): NIST's NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The website contains resources for workforce development (including the NICE Cybersecurity Workforce Framework documented in NIST draft Special Publication 800-181, which provides a taxonomy for classifying cybersecurity roles), educational activities and programs, and other materials and resources that support cybersecurity training.

NIST NICE

CAE-CD: The CAE-CD program is jointly sponsored by NSA and DHS. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation. All regionally accredited two-year, four-year, and graduate level institutions in the U.S. are eligible to apply to be designated as a two-year, four-year, or research CAE-CD. Prospective schools are designated after meeting stringent CAE criteria and mapping curricula to a core set of cyber defense knowledge units or specialized focus areas. The CAE-CD website has a list of the current academic centers of excellence, as well as the curriculum requirements and additional resources to help map curricula.

NSA and DHS CAE-CD

DHS Cyber Storm Exercises: DHS conducts the Cyber Storm exercises every two-years to strengthen cyber preparedness in the public and private sectors. The exercises follow the training theory of "train like you fight, fight like you train", allowing participants to exercise decision-making, coordination, collection, response and recovery to validate actual readiness. Cyber Storm V, in part, focused on the HPH Sector.

DHS Cyber Storm Cyber Storm: Securing Cyber Space

Appendix D: Cybersecurity Best Practices from Other Critical Infrastructure Sectors

To address subsection A of the Act section 405 (c) to analyze how industries, other than health care, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries, the HCIC Task Force received briefings from members of the Financial Services and Energy Sectors. Both the Financial Services and Energy Sectors share similar cyber threat profiles with the HPH Sector, and as such are well-suited to serve as a basis for comparison of cybersecurity risks and challenges.

The Task Force agrees with leveraging shared resources, personnel, and capabilities, similar to what the Financial Services Sector has implemented. However, the Task Force found that some of the unique aspects of the health care industry would prevent the direct adoption and implementation of these practices: 1) size and diversity of the industry; 2) forced digitization; 3) reliance on legacy systems; 4) delays in identifying threats; and 5) the number of highly-interconnected systems in health care vs. the number of closed systems present in the Financial Services and Energy Sectors.

Financial Services Sector

Similar to the HPH Sector, Financial Services faces a growing set of cybersecurity risks as adversaries multiply, insurance businesses continue to play an integral role in people's lives, and IT becomes more a ubiquitous part of daily operations. Additionally, like the HPH Sector, the Financial Services Sector struggles with the diversity of needs within the sector and the high level of inter-connectedness within the industry. The structural factors underlying how customers engage financial institutions, how those institutions interact with one another, data sharing, and how IT facilitates these transactions play a large role in shaping cybersecurity risks.

These risks reflect the interconnection of financial, reputational, regulatory, and business continuity impacts produced by nation states, organized criminals, and hacktivists. Reportedly, most financial institutions have experienced attempted or successful intrusions into their IT systems between 2011 and 2014.[74] Because the Financial Services Sector is positioned at the center of a web of dependencies across nearly all critical infrastructure sectors, it is a particularly appealing target for nation state actors motivated by any number of political, economic, or military objectives; organized criminals who target the sector for primarily economic reasons; and politically motivated hacktivists.

Like the HPH Sector, the Financial Services Sector faces serious issues with the error category of threat action. Financial Services also faces challenges in preventing abuse or misuse of systems, which range from security policy violations, to bring your own device allowances, to third party risks emanating from the heavily interconnected nature of entities in the financial ecosystem. [75]

[74] New York State Department of Financial Services. (2014). *Report on Cybersecurity in the Banking Sector*. Retrieved from: Cybersecurity in banking sector

[75] Vijayan, J. (2015). *Security Spending and Preparedness in the Financial Sector: A SANS Survey*. Retrieved from Security spending in financial sector

Energy Sector

Similar to the HPH Sector, the characteristics of cyber risk in the Energy Sector reflect the dynamics of how data flows and IT systems connect businesses and customers. At its inception, the Energy Sector was not intended to connect to the Internet. However, the resulting connection to business networks created unintended threats and resulted in the need for increased cybersecurity. Because the Energy Sector is foundational to the operation of all other critical infrastructure sectors, it is an especially significant potential target for threat actors. Nation state motivations in conducting cyber operations against the sector can span the entire political, economic, and military spectrum. While nation states often target energy extractive industries, such as oil and natural gas companies to steal of intellectual property, an attack designed to cripple utilities and destroy assets for energy generation, transmission, and distribution remains a tremendous risk.

With the advent of "smart" industrial control systems and the integration of IT into the operational side of the Energy Sector, cyber risks will continue to increase. In 2016, approximately 73 percent of IT security professionals at utilities companies acknowledged that adversary actions had caused a public security breach.[76] Whether working to use new IT systems and devices, integrating legacy hardware and software, or maintaining operations, both the HPH and Energy Sectors broadly share a set of characteristics. The highest-level risks in the Energy Sector encompass destruction of critical infrastructure, threats to life/safety, and regulatory and reputational impacts.

Lessons Learned and Best Practices Application

The Financial Services and Energy Sectors apply five key areas to address cybersecurity-related challenges. The table below summarizes key statistics and findings for each sector:

Table 19 Lessons learned and best practices

Best Practice	Why is it Helpful?	Financial Services Sector	Energy Sector
Information Security Governance	Information security governance outlines the many components that make up the controls and procedures required to systematically address cybersecurity issues and manage risks.	Approximately 90 percent of institutions have an information security framework that includes: (1) a written information security policy; (2) security awareness education and employee training; (3) management of cyber risks and inclusive of identification of key risks and trends; (4) information security audits; and (5) incident monitoring and reporting.	Roughly 46 percent of institutions follow standardized incident response practices, 40 percent provide security awareness and employee training, 60 percent conduct regular information security audits, and 54 percent have well-documented processes for incident response and tracking.

[76] CISCO. (2016). *Utility and Energy Security: Responding to Evolving Threats*. Retrieved from: Utility and energy threat response

Best Practice	Why is it Helpful?	Financial Services Sector	Energy Sector
Information Sharing Organizations	Cybersecurity requires ongoing coordination and collaboration between those who experience threats and those who design and implement solutions. Information sharing is crucial to increase threat awareness and mitigate overall risks.	Approximately 60 percent of large institutions, but only 25 percent of small institutions, participate in an information sharing organization to track and disseminate data on cybersecurity threats and vulnerabilities. The Financial Services Information Sharing and Analysis Center serves as the largest source of information for the sector by providing resources from the government, subscription feeds, and information from member companies and other Information Sharing and Analysis Centers. The Information Sharing and Analysis Center has circles of trust and thousands of information sharing groups that discuss issues (such as intrusions and vulnerabilities) and the largest banks share reporting issues and best practices.	Only 41 percent of institutions rely on industry information sharing partnerships as a source of cybersecurity intelligence on threats and vulnerabilities. This reluctance to share data with public and private sector institutions may stem from concerns regarding the potential regulatory compliance actions, potential privacy or antitrust liability, and possible public disclosure of information.
Security Technology	Security technologies provide critical capabilities with which organizations can to defend against, monitor, detect, isolate, and log cyber threats.	The vast majority of institutions reported using the following tools: anti-virus software, spyware and malware detection, firewalls, server-based access control lists, intrusion detection tools, intrusion prevention systems, vulnerability scanning tools, encryption for data in transit, and encrypted files.	The majority of institutions reported using the following tools: anti-virus/anti-malware software, physical access controls to control systems and networks, zones of network segmentation, monitoring and log analysis, technical access controls, asset identification, risk assessments and audits, and firewalls.
Security Assessments	Conducting regular assessments of the assets and connections within a network helps to establish a baseline of operations to	Penetration tests are conducted industry-wide, with 100 percent of large and medium institutions and 91 percent of small institutions undertaking such testing. Roughly 80	60 percent of institutions conduct regular security assessments or audits in order to better understand the status of and protect control systems.

Best Practice	Why is it Helpful?	Financial Services Sector	Energy Sector
	detect cyber threats and vulnerabilities.	percent of institutions do so on an annual basis. The sector leverages the Hamilton Exercise to deal with product lifecycle threats from identification to recovery.	
Third Party Vendor Management	Because an entity's cybersecurity is as strong as its weakest link, managing threats to third parties is critical to an entity's overall risk profile.	84 percent of the broker-dealers and 32 percent of the advisers require cybersecurity risk assessments of vendors with access to their firms' networks.	Roughly 65 percent of institutions consider third-party vendor qualification of security technologies or solutions to be highly important or mandatory, but only 58 percent are partially vetting third parties.

Additionally, subject matter experts from the Financial Services and Energy Sectors identified the following leading practices to prevent and manage cybersecurity risks:

- **Conduct Comprehensive Information Sharing**: To manage risks appropriately, organizations need the highest quality information available. Gaining increased insight into current threats, attack vectors, and the systems within the enterprise will increase an organization's ability to detect and prevent threats, as well as increase the understanding of inherent risks.

- **Implement Baseline Protections**: Organizations can take multiple steps to increase the security of their infrastructure to include patching against known vulnerabilities, implementing additional controls to support cyber efforts, deploying industry-accepted best practices, and understanding how those practices protect systems. To promote baseline protections, industry must communicate that information in a way that is understandable to the consumer and prompts organizations to take decisive actions to implement the baselines.

- **Design and Test Response and Recovery Efforts**: Even with quality information and baseline protections in place, incidents will continue to occur. Critical to response and recovery efforts is the development of response plans and the testing and exercising of response activities to understand how the organization will identify and react to incidents. Testing these responses will enhance the ability to respond during a crisis through established mechanisms and defined actions, as well as provide structure and chain of command when communicating with trusted sources to assist in response efforts.

- **Enhance Communications and Collaboration**: Increasing information sharing and communications will improve sector-wide awareness of risks, and will enhance holistic threat analysis capabilities. Engaging in more regular and formalized collaboration will also serve to educate a larger portion of the sector that may not otherwise have access to information about the latest threats.

Appendix E: Acronyms

ASPR	Assistant Secretary for Preparedness and Response
CAE-CD	National Centers of Academic Excellence in Cyber Defense
Act	*Cybersecurity Act of 2015*
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
DHS	U.S. Department of Homeland Security
EHR	Electronic Health Record
FBI	Federal Bureau of Investigation
FDA	U.S. Food and Drug Administration
FTC	Federal Trade Commission
HCIC Task Force	Health Care Industry Cybersecurity Task Force
HHS	U.S. Department of Health and Human Services
HIMSS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HPH	Health Care and Public Health
IoT	Internet of Things
IT	Information Technology
ISAO	Information Sharing and Analysis Organizations
MedCERT	Medical Computer Emergency Readiness Team
MSSP	Managed Security Service Provider
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
OCR	Office for Civil Rights
ONC	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
R&D	Research and Development
SDL	Secure Development Lifecycle
SDLC	System Development Lifecycle
U.S.	United States