HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

February 3, 2017

DRAFT#2

PRE-DECISIONAL NOT FOR DISTRIBUTION

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

Members of the Task Force

Commented [JC1]: Members should send any corrections to title or certifications to: jcentola@deloitte.com

The following 21 individuals constitute the membership of the Health Care Industry Cybersecurity Task Force.

- **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
- **Laura Laybourn,** Director, Stakeholder Engagement and Cyber Infrastructure Resilience, Office of Cybersecurity and Communications, U.S. Department of Homeland Security
- **Kevin Stine,** Chief, Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology
- **Joshua Corman,** Co-Founder, I Am The Cavalry
- **George DeCesare, JD,** Senior Vice President and Chief Technology Risk Officer, Kaiser Permanente Health Plan
- **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
- **Michael McNeil,** Global Product Security and Services Office, 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 (Becton, Dickinson and Company)
- **Christine Sublett, MA, CISSP, CIPS, 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, Dr. Aftin Ross, Thad Odderstol, Jason Cameron, Donna Dodson, Ben Flatgard, Major William Marsh, Kathryn Martin, Nickol Todd, Stephen Niemczak, Lucia Savage, Adam Sedgewick, Malikah Smith, Richard Struse, Scott Vantrease, Mark Weber, Nicole Edison, Margie Zuk, Penny Chase, Darren Leitsch, Joanna Centola, Ken Trumpoldt, Ryan Marinella, and Chris 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 efforts to establish and support the Task Force throughout its efforts.

Date

To “appropriate congressional committees”,

INSERT COVER LETTER

Sincerely,

Contents

This page intentionally left blank.

Executive Summary

Commented [JC2]: Under development

Within the *Cybersecurity Information Sharing Act of 2015*, Congress established the formation of the Health Care Industry Cybersecurity Task Force to address the challenges the health care industry faces securing against Cyber attacks.

Within the health care industry, serving and providing the best patient care is the highest priority and health care providers spend a majority of their funding and personnel resources to helping as many patients as possible; in effect, patient lives outweigh security and privacy concerns. Cybersecurity has historically been viewed as an IT challenge, approached reactively, and often not seen as a solution that can help to protect the patient. Limited financial resources in all but the largest organizations and a general lack of understanding of cybersecurity risks increase the challenge to prioritizing cyber initiatives within the health care industry. Members of the health ecosystem reported that without experiencing a breach or data loss, many security professionals and organizations have difficulty demonstrating the importance of implementing cyber protections and how proactive risk mitigation can save the organization money and reputational damage in the long-term. Making the decision to prioritize cybersecurity within the health care environment will require organizational culture shifts and increased communication from leadership, as well as changes to the way providers perform their duties in the clinical environment.

Health care data may be used for a variety of nefarious purposes including, for example: fraud, identity theft, the theft and sale of proprietary information, and disruption of hospital systems and patient care. A significant challenge and vulnerability for providers, hospitals, pharmaceuticals, 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. As such, securing health care data and medical devices is an essential component to protecting patients and providing them with the highest level of care. If left unchecked, the probability that a cybersecurity threat will cause a significant loss of life or harm will increase. It is also entirely possible that multiple, individual events have already occurred and are going either entirely unnoticed.

While prescribing a medicine or implanting a medical device, no doctor considers their reliance on manufacturing control processes or quality checking schemes used to make those medicines or devices, yet all meta tools for manufacturing are now digital. Today, many doctors focus on clinical processes; many physicians process and accept payments without needing to consider the tremendous digital health databases that insurers must maintain to ensure proper payment. Increasingly, doctors expect to gain instant or near instant access to the data maintained in those remote systems. Except for IT staff, providers and other health care workers assume that the IT network and the devices they support function flawlessly and that their level of cybersecurity vulnerability is extremely low.

While no organization has all the financial resources it needs to employ all the personnel necessary to consistently and confidently protect its networks and data, many larger organizations have the capacity to, at the very least, employ security professionals (e.g., Chief Information Security Officers, Chief Information Officers) who have the responsibility to implement security measures across the enterprise. In contrast, many small organizations: cannot afford to retain in house or qualified security personnel; have designated cybersecurity personnel with multiple areas of responsibility outside of cybersecurity; lack the infrastructure to identify

and track threats; and lack the capacity to analyze vulnerability data they receive and translate it into actionable information. In effect, these organizations fall below the "technology and security poverty line" and may not know they have experienced an attack until long after it has occurred. For both large and small organization, a large number of unsupported legacy devices exist which cannot be easily replaced.

The Task Force organized their recommendations into seven main Imperatives.

- Develop the health care workforce necessary to prioritize cybersecurity awareness and technical capabilities.
- Enhance cybersecurity across the interconnected health care ecosystem.
- Increase the prevalence of and access to cybersecurity awareness and educational programs across health care industry stakeholders.
- Improve sharing and usage of cybersecurity information throughout the entire health care industry.
- Consider the unique challenges for health delivery organizations and small providers and develop incentives to increase overall cybersecurity posture.
- Increase the security and resilience of medical devices and health technology.
- Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.

I Health Care Industry Cybersecurity Task Force Charge and Approach

Despite political and ideological differences, concerns and issues related to cybersecurity figure prominently into the platforms of both the Republican and Democratic parties. As such, Congress passed the *Cybersecurity Information Sharing Act of 2015* (CISA or the Act). Given the severity of attacks in recent years and the rapid universal deployment of information technology throughout the health care environment, Congress singled out the health care industry in CISA and required the establishment of the Health Care Industry Cybersecurity (HCIC) Task Force. Under Section 405 (c), CISA required the Task Force to accomplish six tasks culminating 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*[1] was a call to arms for patient safety, the Task Force hopes that this report galvanizes both the public and private sector to comprehensively address the vulnerabilities in health information technology in order to protect patients.

One of the most critical challenges that the Task Force heard from subject matter experts, briefings, survey results, and public blog posts was related to resources. The majority of health care providers and a substantial portion of other stakeholders in the health care industry reside on the wrong side of a "cybersecurity digital divide". Most of the health care in the U.S. is provided by smaller practices, hospitals, and organizations. Operating margins can still be under one percent profit, and critical access hospitals struggle to stay open. As care has expanded in the ambulatory venue, this has become more problematic for physician offices that are small and often isolated. If every health care organization was required to followed cybersecurity best practices tomorrow, many would be forced to choose between procuring new security technologies and related subject matter expertise, or purchasing new ventilators and hiring nurses.

Commented [JC3]: Do we need a citation for this term?

A. Analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries

The HCIC Task Force received briefings and gathered information from other sectors such as the Banking and Finance, Transportation, and Energy Sectors. Appendix C summarized the public and private meetings schedule of the Task Force.

B. Analyze challenges and barriers private entities (notwithstanding section 102(15)(B), excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks

The challenges and barriers, as described in detail in this document, center around several themes: resources for implementation at the provider level, lack of standardization of platforms, legacy systems, regulatory concerns including antitrust, and the foundational problem of balancing security and privacy with access and the free flow of information. In addition, there are proprietary issues for private entities. Additionally, the Healthcare

[1] Institute of Medicine. (1999). *To Err is Human: Building a Safer Health System*. Retrieved from: http://www.nationalacademies.org/hmd/~/media/Files/Report%20Files/1999/To-Err-is-Human/To%20Err%20is%20Human%201999%20%20report%20brief.pdf

and Public Health (HPH) Sector represents approximately 10 percent of the total United States (U.S.) workforce.

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 (EHR)

Even if Congress was willing to provide multi-billion support to secure the digital resources in health care, there are simply too few people with the combined expertise in both health care technology and cybersecurity to meet the current demand. It is clear to members of the HCIC Task Force that we still need substantial funding for health care cybersecurity. Such funding needs to be focused substantially on developing highly efficient, cost-effective, resilient solutions health care solutions that provide effective defenses health care networks. For further information about other challenges and barriers to the health care industry, see Section III Challenges and Barriers to Securing the Health Care industry.

D. Provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry

The Task Force identified the previously developed materials for use by industry (see Appendix E. Resource Catalog) and proposed the creation of new educational and awareness materials targeting health care executives, boards, and medical staff (see Section VI Imperatives, Recommendations, and Action Items). It has been well established that to ensure competency one must educate and train, and not just distribute manuals therefore merely providing advanced cybersecurity study materials will not create thousands of cybersecurity experts or lead to increased security of an organization's systems and technology-based assets. The HCIC Task Force believes that increasing the amount of, and access to, educational and awareness information is a fundamental component of helping the sector increase security while meeting the ultimate goal of providing patient care and ensuring patient safety. However, the Task Force also recognizes that most of the available information will not help to advance security without personnel who are in a position to understand, apply, and implement those educational resources.

E. Establish a plan for creating a single system for the Federal Government to share information on actionable intelligence regarding cybersecurity threats to the health care industry in near real time, requiring no fee to the recipients of such information, including which Federal agency or other entity may be best suited to be the central conduit to facilitate the sharing of such information

The HCIC Task Force made a considerable effort to contemplate the most effective means by which to create a single system to share actionable intelligence. The Task Force recognized that it is more difficult than anticipated to create an environment inside a health care organization that can quickly answer the question, "Does this threat information apply to me?" The Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) and the Office of the Assistant Secretary for Preparedness and Response (ASPR) funded the Information Sharing and Analysis Organizations (ISAO) that provided a target for our

Commented [JC4]: Need a citation here

Commented [JC5]: Comment from Theresa: This section does not have any content about networked medical devices/EHR. I think this is in the wrong place. It is a discussion about workforce

recommendations. This allowed us to develop specific strategies and tactics that should make threat sharing more effective. Section VI includes recommendations related to sharing threat information, such as specific policy changes to ensure that health care organizations can affordably share data without fear of liability from regulation or litigation. It also includes tactics to ensure that threat information is useful.

Additionally, threat sharing information cannot, and should not, be separated from cybersecurity training efforts. The Task Force believes that no threat information should be disseminated without the corresponding information required to provide context for that threat information. Providing this additional context is a way to promote ongoing training of health care industry stakeholders and to deliver current and timely information that recalibrates in response to shifting threats.

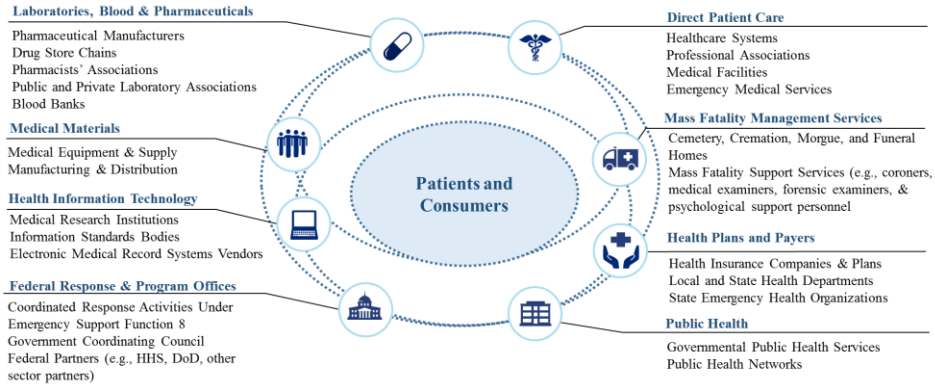
II The State of Cybersecurity within the Health Care Industry

Commented [JC6]: Under revision to consolidate

Organization of the Health Care Industry

The HPH Sector Coordinating Council and Government Coordinating Council define the health care space in their 2016 Sector Specific Plan and as illustrated in Figure 1 below. The document defines the sector 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."[2]

Figure 1. Health Care Ecosystem



In consultation the Director of the National Institute of Standards and Technology (NIST) and Secretary of Homeland Security, the Secretary of Health and Human Services (HHS) brought together a diverse group of industry representatives consistent with requirements as outlined in

[2] *Healthcare and Public Health Sector-Specific Plan*. (2016, May). Retrieved from: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

CISA.[3] Additional input for this report was gathered through engagement with leading industry organizations and public comments.

Health Care has a Unique Culture

Within the health care industry, providing the highest level of patient care is the priority and providers spend a majority of their funding and personnel resources to help as many patients as possible; in effect, patient lives outweigh security and privacy concerns. Due to the critical role that members of the health care ecosystem play in the lives of all patients, information sharing and cybersecurity are generally not seen as a priority for practitioners or other care providers. To allow health care staff to respond to critical care issues quickly and maintain a seamless workflow, personnel may leave workstations unlocked and unattended to retain access to patient information and to share data between groups and departments to provide comprehensive care. While this improves the speed with which a provider can access the patient's information and identify potentially lifesaving allergies or drug interactions, these common practices can lead to loss or unauthorized alteration of patient data.

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

Cybersecurity Challenges within Health Care are Extensive

The digitization of the health care industry created a new challenge for cybersecurity in health care where protecting patient data, in addition to ensuring patient safety, becomes a measure of success. Health care data may be used for a variety of nefarious purposes including, for example: fraud, identity theft, the theft and sale of proprietary information, and disruption of hospital systems and patient care. A significant challenge and vulnerability for providers, hospitals, pharmaceuticals, 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. As such, securing health care data and medical devices is an essential component to protecting patients and providing them with the highest level of care. If left unchecked, the probability that a cybersecurity threat will cause a significant loss of life or harm will increase. It is also entirely possible that multiple, individual events have already occurred and are going either entirely unnoticed. Additionally, ransomware or a denial of service attack coupled with a mass casualty event, such as an explosive device, would cripple the ability of the health care organizations to respond.

Commented [JC7]: Comment from Theresa: David Ting – This might be a good area to address the flow of patients, visitors and families through our organization.

Commented [JC8]: Comment from Jacki: Are we defining practitioners to be clinicians? I think we need to broaden this out if yes and also contemplated other factors like lack of funds, lack of education, legacy systems that were designed for cyber attacks, etc.

[3] CISA includes: 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 stakeholder.

If patients are to develop and sustain trust in the digital component of the health care system, we must prioritize practical cybersecurity thinking across the continuum of health care. Such thinking can help to shift cybersecurity from solely a leadership and IT priority to a much broader cultural change that is pervasive across the organization to protect patients from digitally-sourced harm. A new element that extends the scope of the problem is access to health records and importing of data into those records by patients. The myriad of applications that are being developed or utilized to allow patients to participate actively in their own care extends the vulnerability way beyond the 14 million workers involved in health care in the U.S.

Health Care Has Undergone a Digital Transformation

The last decade has witnessed the health care industry adopting EHRs as a standard tool for documentation and workflow. In the last few years they have connected these digital systems to the Internet and realized the benefits and consequences that can result from that level of interconnectivity. This transformation highlights not only the size of the sector and breadth of services provided, but also the disparity within health care as digital transition has occurred at different paces and at different times, with a majority of the sector making finical investments in cybersecurity only within the last five years.[4] While the health care industry faces many of the same threats as other industries (e.g., lack of qualified security staff, prevalence of small and medium-sized businesses), health care is approximately a decade behind certain key sectors such as Financial Services that have demonstrated an advanced understanding of cyber threats while implementing effective protective mechanisms.

Medicine has been using digital systems for many years, especially for administrative functions, such as billing, yet remained surprisingly disconnected. We are easily changing the connectivity of digital connectivity more in this decade than the last 30 years combined. This connectivity increases the dependence on technologies that support lifesaving and life maintaining operations; any challenge or change to integrity or availability settings (e.g., malfunctioning IV pump, uncalibrated nuclear medicine device) has the potential to harm patients. 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 intended to be Internet accessible or was not designed to resist cyber attacks.

Similarly, the volume of connected medical devices and automated medication delivery systems has increased. In some cases, mere connectivity between two devices such as a glucose monitor and an insulin delivery system can provide profound new benefits to both health care professionals and patients. However, if not protected, this interconnection could pose a risk to patient safety. Modern implantable devices are expected to go beyond therapy and produce actionable data for users. Like the digital machines discussed above, most medical devices were not designed to frequently communicate with users; nevertheless medical device owners are anxious for whatever data they can obtain. Therefore, securing health care data and medical devices is essential to protecting patients and providing them with the highest level of care.

While prescribing a medicine or implanting a medical device, no doctor considers their reliance on manufacturing control processes or quality checking schemes used to make those medicines or devices, yet all meta tools for manufacturing are now digital. Today, many doctors focus on clinical processes; many physicians process and accept payments without needing to consider the

Commented [JC9]: Need to bring EHRs and IoT into the discussion

Commented [JC10]: Under development: Include conversation about supply chain

Commented [JC11]: Comment from David Ting: How do we quantify being a decade behind?

Commented [JC12]: Comment from Jacki: I think we should add the push for inoperability somewhere in here.

Commented [JC13]: Comment from David Ting: Not sure what is meant by not communicating with users – many of the integrated devices can be managed using smartphones or dedicated devices. Many patient devices can, however, send their data to the cloud. Is this what we are trying to say?

[4] Institute for Critical Infrastructure Technology. (2016). *Hacking Healthcare IT in 2016*. Retrieved from: http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf

tremendous digital health databases that insurers must maintain to ensure proper payment. Increasingly, doctors expect to gain instant or near instant access to the data maintained in those remote systems. Except for IT staff, providers and other health care workers assume that the IT network and the devices they support function flawlessly and that their level of cybersecurity vulnerability is extremely low.

Cyber attacks to the health care industry can cause issues directly affecting patient safety and care. Imagine how a medium-sized medical device manufacturer might be forced to abandon development of a new, life-saving device due the theft of their research and development (R&D) data, or a cyber attack directed at an EHR. Similarly, theft or corruption of academic research data might produce results that can lead to patient harm. As stated before, the security of the entire health care enterprise is a patient safety issue. While some cybersecurity threats could result in damaging impacts over a long period of time, there are also cybersecurity threats that will have impacts in just minutes or seconds. To protect patient safety, we must learn to defend against all time scales.

Cybersecurity Risks Increased Due to a Cascade of Market Failures

The health care industry, for multiple reasons, was very slow in embracing information technology, requiring the Federal Government to subsidize the adoption of EHRs. All other industries did so over the course of decades, organically determining what processes would benefit from automation. Technology in other industries typically co-evolved with some awareness of the cybersecurity threats to their technical infrastructure. In the recent past, any data leaving a system or provider space had to be printed and any documents had to be read and transcribed before being ingested. In that way the health care industry was protected from cyber threats because it is difficult to hack a system that you can only communicate with using paper documents. But a market failure of health care ensured that automation was limited to the rare cases where health care providers benefitted financially from automation of technology. The sharing of data with patients, or with other providers on behalf of patients was not supported by financial benefits. Digital record keeping was limited to the data required to demonstrate that medical billing occurred correctly. A more recent health care cybersecurity strategy was simply to keep all digital data in-house, behind the "firewall" in all circumstances, regardless of what damage this did to the patient's care.

However, years of avoiding automation has resulted in rising health care costs that contribute to a steadily growing percentage of our national GDP. As health care costs continued to threaten the U.S. economy, it became apparent to policy makers that a digital intervention was required. The health care delivery system was shocked with multiple parallel imperatives that have dramatically increased the number of public-facing Internet services required for them to operate. These include:

- Funding for digital technology for doctors in the Meaningful Use and the *Medicare Access and CHIP Reauthorization Act* (MACRA) incentives;
- Increased patient access to digital lab data;
- Requirements for digital access to data for patients inside the *Health Insurance Portability and Accountability Act* (HIPAA);
- Increased remote monitoring and reporting systems for medical devices; and
- Data requirements of personalized medicine, especially for cancer treatment.

Commented [JC14]: Include EHR drivers and Changes with EHRs helped push the industry to digitize.

Commented [JC15]: Comment from David Ting: What is the "market failure of health care"? Agree with the statement that HC was slow in digitizing their data to facilitate faster information exchange – this coupled with the lack of experience in cyber security leads to an easy attack surface

Comment from Theresa Meadows: Not sure how to interpret – potential to delete unless further explained.

Commented [JC16]: Comment from David Ting: When EHRs were introduced HIPAA came in to enforce privacy of the PHI = not the security of the system delivering care. This point, perhaps, might be important as only now, post MU2 is the attention being paid to CS.

Commented [JC17]: Need a citation

These changes resulted in an increase in the available attack surface of health care providers, medical device companies, and many other parts of the health care industry. Patients and physicians have derived many benefits from digitization to include a patient's ability to access their information through portals and the ability for providers to more easily share patient information. However, these interoperability efforts may have increased risks to patients due to the introduction of unsecure solutions such as a patient portal accessible over the public Internet with only limited security controls in place. Although the Centers for Medicare & Medicaid Services (CMS) was willing to pay providers for "having" a patient portal, there was no universal standard for cyber safety. Additionally, the rapid expansion of EHRs was accomplished with multiple vendors with minimal standardization of security best practices.

The revolutionary pace of adoption of EHRs was a success, but this is the time to pause and have the Congressional support to fortify the cybersecurity foundation of the health care industry. This will require an unparalleled public-private partnership.

Health Care Delivery Comes From Organizations and Providers of All Sizes

The health care industry is unevenly prepared for the current sophistication and diversity of cyber threats. In addition to the tremendous variety of services provided, organizations within the health care industry are widely diverse in terms of size. Large academic institutions and health delivery organizations take cybersecurity risks seriously and have many resources in place to protect their systems. However, today most health care is still delivered by smaller practices and small rural hospitals that do not have the resources to protect themselves from an ongoing threat that changes tactics and attack vectors quickly. As a result, many small organizations: cannot afford to retain in-house or qualified security personnel; have designated cybersecurity personnel with multiple areas of responsibility outside of cybersecurity; lack the infrastructure to identify and track threats; and lack the capacity to analyze any threat data they receive and translate it into actionable information. Many of these organizations also: lack physical and logical access controls; continue to use unsupported legacy systems; use default passwords; and lack access to proper security training. In effect, these organizations fall below the "technology and security poverty line" and may not know they have experienced an attack until long after it has occurred.

Commented [JC18]: Comment from Emery: Need to determine phrasing consistency – digital divide vs. poverty line.

Is there a citation for this term?

While no organization has all the financial resources it needs to employ all the personnel necessary to consistently and confidently protect its networks and data, many larger organizations have the capacity to, at the very least, employ security professionals (e.g., chief information security officers [CISO], chief information officers [CIO]) who have the responsibility to implement security measures across the enterprise. Large organizations and provider networks also have more financial resources to implement protective mechanisms for a larger percentage of their assets, have the ability to ingest information and threat data, and are able to make the information actionable – which leads to a more resilient security posture.

The general perception is that only larger organizations are the target of cyber attackers due to the volume of sensitive, confidential, or proprietary information that they possess; in reality, health care organizations of all sizes are targets due to the interconnected nature of the environment. Larger health delivery organizations often provide IT services to their affiliates or smaller hospitals; often these connected clinics lack sufficient IT security, but can present a security vulnerability because they are the front-end environments for the EHRs. These risks and issues will continue to grow as the sophistication of attackers and attack vectors continues to

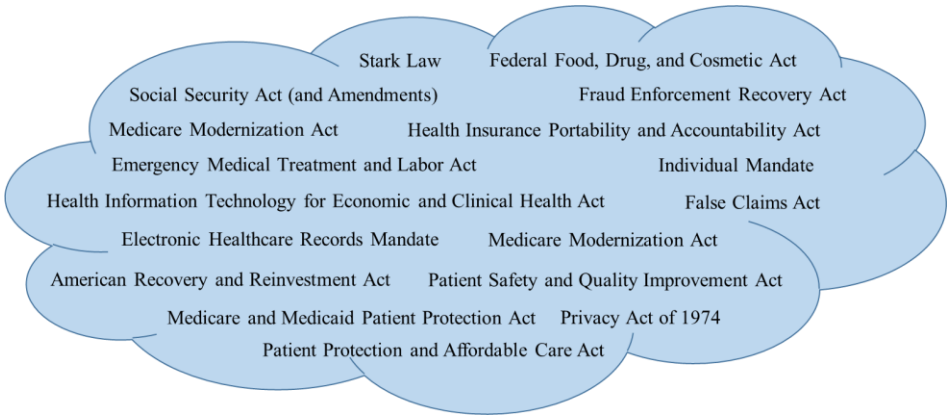
increase, and while IT and security budgets remain flat or decrease due to the number of competing priorities within the environment.

The Health Care Regulatory Environment is Complex

Almost every aspect of the health care economy has to adhere to and comply with a number of regulations, guidance, and mandates. However, at the time of their drafting and passage, these regulations could not have predicted or taken into account the evolution and progression of modern cybersecurity threats. Additionally, the current regulatory frameworks do not allow the health care industry to deal with the wide variety of issues and segments of the sector in a simultaneous manner. Moreover, there are regulatory boundaries at the interface of medical device and health IT connectivity. The movement of electrons across devices and systems do not recognize what can sometimes be artificial regulatory boundaries between product areas. The cybersecurity of medical devices is regulated by the Food and Drug Administration (FDA) under its Quality Systems Regulations (QSR) and these devices may exchange data with EHRs and other health IT whose cybersecurity may be regulated by the Office of the Civil Rights (OCR) and/or the Office of the National Coordinator (ONC). Further there are other applications and technology leveraged in health care that raise cybersecurity concerns which are not regulated or reviewed by any government agency. These are challenges that the health care industry and lawmakers will continue to face when drafting cybersecurity policies and regulations as what is written today will face the same problem of yet unknown threats in the future. Thus it is important that going forward stakeholders consider an agile approach to cybersecurity regulation and guidance within the HPH Sector.

Figure 2. Regulatory Environment for the Health Care Industry

Commented [JC19]: Placeholder graphic. Awaiting graphic to cover health care regulations.



An additional challenge is that the regulations for medical devices and health IT moves slower than the pace of product innovation. As a result, cybersecurity innovations outside of the health care industry move faster than innovations within in health care. Many regulations that apply to cybersecurity in health care are well meaning and individually effective. But taken together they may form a substantial legal and technical burden on health care organizations. Some of these challenges include continually reviewing and interpreting multiple regulations, some of which are vague and/or redundant, and dedicating costly human and technology resources to implement policy directives that in many cases may not have a material impact on reducing risks. This

burden is evidenced by health care systems that are providers, insurance companies, research institutions, and institutions of higher education. FDA in the release of its medical device pre- and postmarket cybersecurity guidance's, has tried to provide a framework that allows device manufacturers to address cybersecurity vulnerabilities in an agile and expedient manner. This complex mosaic results in potential conflicting regulations from multiple oversight bodies.

Health care organizations spend a great amount of time and resources cross-walking all the recommendations from various Federal and State entities. This complexity leads to the potential of misinterpreting or omitting key regulations from daily practice. For example, many organizations assume the measures they have in place for HIPAA with protect them from cybersecurity attacks. This lack of understanding can lead to poor cybersecurity practices.

The Value of Health Care Data Increases over Time

Commented [JC20]: Include discussion of stock manipulation as a driver (ex: St Jude's)

While every industry faces cybersecurity threats, the threats to the health care industry are magnified in part due to the accelerated IT deployment. Patient health data is also largely permanent, while other types of data are not. Credit cards, phone numbers, social security numbers, and even addresses can change when personal data is stolen. Health care data is one of the rare types of personal data that one cannot change and that increases in value with time. A malicious attacker can steal a person's genome today, which could be worth a significant amount of money when scientists can fully decode and understand the data. A teenager's medical history and previous health issues can be stolen today, but becomes valuable when the individual achieves a more prominent role such as becoming mayor or police chief. These differences in value are regularly reflected in the prices for medical records available for sale on the dark web.[5] The general standard across many sectors is to provide one-year of credit protection following a breach or personnel or financial information. However, one-year of identity protection does not provide the consumer[6] with adequate protections based on the sensitivity, value, and permanence of health care data.

While policy decisions require that patients participate in health care technology, many patients have no insight into the potential risks that stem from EHRs or the risks that can result from a successful cyber attack. Based on these factors, it is entirely possible that a catastrophic cybersecurity event will cause a nationwide crisis of patient confidence in the health care system. A loss of trust can be as destructive and harmful as a natural disaster or man-made event (e.g., nuclear attack), but it plays out over the course of decades rather than minutes or hours.

Commented [JC21]: Fred to get info from pubmed about genome markers, etc

III Risks Across the Health Care Industry

Any practitioner, provider network, pharmaceutical company, or device manufacturer will say that their primary priority is providing safe, high-quality patient care, ensuring the efficacy of their drug, ensuring the accuracy of medical records in the EHR, and confirming the reliability of their device. However, there are many underlying risks to confidentiality, availability, integrity, and patient safety that can negatively impact these objectives. Nation states, organized criminals,

[5] Farr, C. (2016, July). *On the Dark Web, Medical Records Are a Hot Commodity*. Retrieved from: https://www.fastcompany.com/3061543/on-the-dark-web-medical-records-are-a-hot-commodity

[6] As used in this report, consumers are patients, beneficiaries, and other individuals that rely on health care services but do not work in or produce products for the health care system.

organizational insiders/partners, and skilled individual hackers understand that cyber attacks yield information that increases in value over time and that some health care subsectors have not implemented strong security practices and do not have personnel with the skills or experience to identify attack or data compromise. Trends in health care such as data consolidation, data integration, and data sharing via EHRs and health information exchanges concentrates data and contributes to an increase in risk. While the rise of EHRs enables new approaches to providing holistic, quality care and analytics, it also creates a ripe target for criminals intending to commit insurance fraud, steal a patient's identity, or manipulate data to cause distrust of the EHR. Furthermore, cyber risks related to medical devices can lead to direct compromises of patient safety.

Commented [JC22]: This isn't the only way to compromise patient safety. Need additional compromises or suggest removal

According to a study by the Ponemon Institute, the most common attacks to the health care industry include exploits of existing software vulnerabilities and web-borne malware attacks. These responses underscore concerns about organizations having neither the awareness of current threats nor the technical personnel in place to prevent these threats, many of which are not new.[7] Additionally, the rise and sophistication of ransomware attacks that hold IT systems and patient-critical devices hostage continues to grow, as evidenced by the ransomware attack on Hollywood Presbyterian Medical Center.[8] In fact, in 2015 this sector had more cyber incidents resulting in data breaches than the other 15 critical infrastructure sectors.[9] More than 90 percent of ransomware attacks on HPH Sector used some variant of the CryptoWall software, which is available for sale online.[10]

While hackers have previously gained access to EHR data through underlying databases, EHR software has not yet been the target of malicious hackers, likely due to the diversity of systems across the ecosystem. The diverse ecosystem of EHR providers has provided an unintended, and almost counterintuitive, benefit and protection for EHR software because no one vendor has become so common across the ecosystem that attacking that EHR specifically would be worthwhile. An additional, unintended protective mechanism for EHRs is that they are isolated and most EHR servers have been firewalled from direct access from the public Internet.

However, regulatory mandates that will force all EHR vendors to have a shared, publicly available API might finally make the EHR software itself into a target for malicious cyber attacks. The goal has been, and should be, for patients to be able to "bring in third-party applications" to gain substantial access to their underlying health care data. However, it is important that HHS generally, and ONC specifically, ensure that the technical details of how to accomplish this are well designed and well deployed, to ensure that this more universal access does not incidentally create a new vulnerable attack surface.

---

[7] Ponemon Institute. (2016, February). *The State of Cybersecurity in Healthcare Organizations in 2016*. Retrieved from: https://cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf

[8] Winton, R. (2016). *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*. Retrieved from: http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[9] Institute for Critical Infrastructure Technology. (2016). *Hacking Healthcare IT in 2016*. Retrieved from: http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf

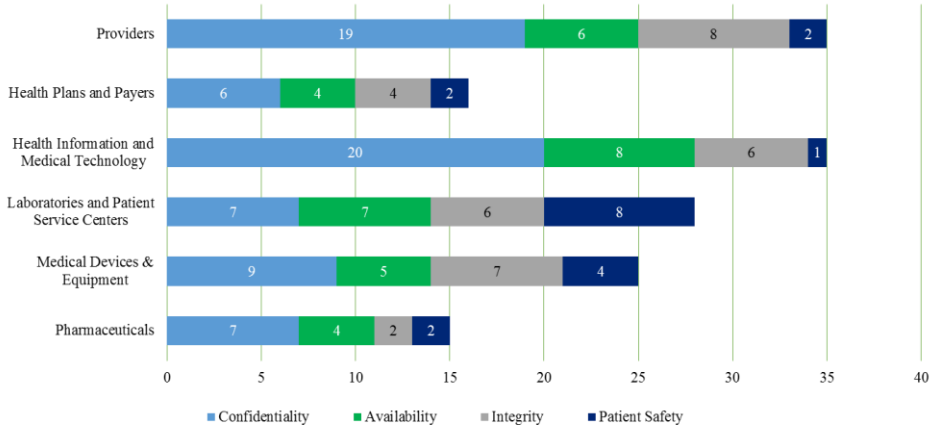
[10] Zetter, K. (2015, August 17). *Hacker Lexicon: A Guide to Ransomware, the Scary Hack that's on the Rise*. Retrieved from: https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/
Green, M. (2016, July 27). *Hospitals are hit with 88% of all ransomware attacks*. Retrieved from: http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html

Health Care Risk Value Chain

In an effort to gather additional information about risks to confidentiality, availability, integrity, and patient safety for some health care subsectors, the Task Force engaged in discussions with personnel from six organizations representing pharmaceuticals, health plans and payers, medical devices and equipment, laboratories and patient service centers, providers, and health information and medical technology. The Task Force collected 151 risks across the value chain (68 confidentiality risks, 30 availability risks, 30 integrity risks, and 23 patient safety). Of the risks identified, 55 percent relate to the loss of protected health information and shared risks across the subsectors included loss or modification of data, disruption of systems or processes, and asset loss or disruption due to software vulnerabilities.

Each respondent specified a business process or corporate function and identified specific risks to those areas. 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. See Appendix F for identified risks. Figure 3 below displays the number of risks each subsector identified in each area of the value chain.

Figure 3. Health Care Subsector Risks Across the Value Chain



Securing Key Health Care Systems

All medical devices carry a certain amount of risk and this includes cybersecurity risks. Medical devices are marketed in the US when there is a reasonable assurance that the benefits to patients outweigh the risks. As more medical devices use software and are increasingly connected to the Internet, hospital networks, and to other medical devices, the risks of potential cybersecurity threats are increased. However, 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 must work to manage them in order to protect patient safety.

Risks to Networked Medical Device and Connected IT Networks

Like other technology, cybersecurity threats and vulnerabilities can impact the confidentiality, availability, and integrity of medical devices and the IT networks they reside on. However, medical devices and the IT networks they are connected to unique in that in addition to data, security, and privacy impacts, patients may be directly impacted by cybersecurity threats and vulnerabilities. Specifically, vulnerabilities and threats to these devices and systems can result in patient harms such as illness, injury, and death. This harm may stem from the performance of the device itself, impeded hospital operations, the inability to deliver care, etc. As a result, addressing patient safety risks are of paramount importance. Table 1 below provides example of cybersecurity risks, which may be related to networked medical devices and their associated IT-networks.[11,12,13,14]

Table 1. Examples of cybersecurity risks to networked medical devices and connected IT networks

	Patient Safety	Availability	Integrity	Confidentiality
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, via malware, etc.)	x	x	x	x
Denial of service attacks which make a device unavailable	x	x		
Exfiltration of patient data or protected health information from the network				x

[11] FDA. (2013). *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*. Retrieved from: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

[12] Deloitte. (2013). *Networked medical device cybersecurity and patient safety: Perspectives of health care information security executives*. Retrieved from: https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/center-for-health-solutions-networked-medical-device-cybersecurity-and-patient-safety.html

[13] FDA. (2016). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[14] Storm, D. (2015). *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks*. ComputerWorld. Retrieved from: http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

	Patient Safety	Availability	Integrity	Confidentiality
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 designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection	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

Management of the risks for medical devices and the IT-networks on which they are integrated is necessary to address safety, effectiveness, and data and system security. Hospitals and medical device manufacturers must therefore leverage comprehensive risk management frameworks which are applied throughout the technology life-cycle of the medical device or IT network. A comprehensive risk management framework enables organizations to take a proactive, risk-based approach to managing their cybersecurity risk and is intended to reduce the risk to patients by decreasing the likelihood that device or network functionality is intentionally or unintentionally compromised by inadequate cybersecurity.

At a macro-level, organizations may leverage the NIST Cybersecurity Framework[15] (i.e., Identify, Protect, Detect, Respond and Recover) to manage their cybersecurity risk. While the

[15] NIST. (2016). *NIST Cybersecurity Framework*. Retrieved from: https://www.nist.gov/cyberframework

NIST Cybersecurity Framework provides a high-level description of standards and best practices to help organizations manage cybersecurity risks, it is not health care industry specific. Thus industry specific guidance for medical device risk management is provided via guidance such as the FDA pre and postmarket guidance for management of medical device cybersecurity which have been aligned with the NIST Cybersecurity Framework.[16,17] Industry specific standards such as *IEC 80001: Application of risk management for IT-networks incorporating medical devices* may also aid health care organizations in defining the roles, responsibilities, and activities associated with managing the risks of their IT-networks incorporating medical devices. In addition to IEC 80001, FDA has also recognized several IT and security standards to aid medical device manufacturers.[18,19,20,21,22,23]

Cybersecurity risk management is an ongoing process which includes identifying hazards associated with the device and/or network, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls that are implemented. A key component of this process is risk assessment and threat modeling plays an important role in this assessment. For medical devices, threat modeling may be used to strengthen security by identifying threats and vulnerabilities for a specific product, across a product line, and within the organization's supply chain to reduce patient safety impacts. A primary purpose of conducting the cyber-vulnerability risk assessment for medical devices is to evaluate whether the risk of patient harm is controlled (acceptable) or uncontrolled (unacceptable). In order to determine the risk, medical device manufacturers should consider the exploitability of the vulnerability and the severity of the health impact to patients if the vulnerability were to be exploited.

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 are connected. Developing a shared understanding of risk assessment enables stakeholders to repeatedly and efficiently assess patient safety, public health, and security risks

[16] FDA. (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

[17] FDA. (2016). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[18] AAMI. (2015). *AAMI TIR57: Principles for medical device security—Risk management*. Retrieved from: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729

[19] Clinical and Laboratory Standards Institute. (2014). *AUTO11-A2 - IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard*. Retrieved from: http://shop.clsi.org/site/Sample_pdf/AUTO11A2_sample.pdf

[20] 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: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57939

[21] 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: https://webstore.iec.ch/preview/info_iec62443-1-1%7Bed1.0%7Den.pdf

[22] 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: https://webstore.iec.ch/preview/info_iec62443-2-1%7Bed1.0%7Den.pdf

[23] 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: https://webstore.iec.ch/preview/info_iec62443-3-1%7Bed1.0%7Den.pdf

associated with identified cybersecurity vulnerabilities and threats. Moreover, doing so allows organizations to take appropriate action to mitigate the risks that may impact patient harm and privacy. Thus it is important that organizations follow industry specific guidance, standards, and best practices which are aligned with the Cybersecurity Framework.

IV Cybersecurity Best Practices from Other Critical Infrastructure Sectors

To address subsection A of CISA section 405, the Task Force received briefings and information from members of the Financial Services, Energy, and Banking 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, as well as the potential adoption of select best practices. However, the Task Force found that some of the health care industries uniqueness' (e.g., size and diversity of the health care industry, forced digitization, reliance on legacy systems, and delays in identifying risks and implementing protections, highly-interconnected vs. closed systems in the Financial Services and Energy Sectors) would prevent the direct adoption and implementation of these practices. For example, the Banking Sector has the advantage of using a shared infrastructure provider model. While the Task Force believes a shared services model could benefit some small and medium size organizations that cannot implement cybersecurity protections on their own, the model implemented by Banking would not work for HPH because Banking has consolidated service providers. In health care, the need exists to leverage shared resources, people, and capabilities.

While the Task Force agreed with the best practices presented by Financial Services and Energy, it developed independent recommendations that will form the basis of allowing the health care industry to implement similar best practices in the future. For additional information on the comparison of the Financial Services and Energy Sectors to the HPH Sector, as well as best practices identified by each sector, see Appendix D.

V Cybersecurity Communications Plan

Commented [JC23]: Under Review to consolidate and align with recommendations

Challenges and Barriers to Health Care Industry Communications

Sharing critical information across multiple entities and stakeholders poses challenges even in the best of circumstances when established communications channels and trusted relationships are in place. Stakeholders within all of the health care subsectors must have the ability to communicate actionable information in real time in response to a changing threat landscape and continually advancing attack vectors. Without such processes and relationships, lines of communications can easily break down resulting in either organizations not sharing information, or communicating incomplete or inaccurate information. This challenge is particularly true in the health care industry due to the breadth of services and stakeholders within the sector.

The size of the health care industry and diversity of its stakeholders constitutes a key communications challenge. Based on the sheer number of organizations within the sector and

variety of services provided, stakeholders can have difficulty determining who to share information with, knowing what types and how much information to share, and understanding when to share it. Organizational size also plays a role in the ability to communicate and ingest information; small and many medium size organizations do not have the ability to either share information or analyze the data they receive due to limited financial or personnel resources. An additional organizational barrier to information sharing is that many organizations and entities within the sector are competitors and fears exist that sharing some information could become a competitive advantage for other organizations. Note – discuss change management regarding fear of repudiation, etc.

Commented [JC24]: Should there be some input regarding the small, non-organizations, such as the single practicing provider or office with 2-3 providers?

Graphic depicting multiple threat sources

While some entities have established relationships with other organizations or industry groups to communicate and share information, these trusted relationships are not in place across the sector or with enough organizations to make the best use of shared information. Additionally, many organizations fear that sharing certain information (e.g., successful attacks and intrusions) could lead to negative repercussions such as brand damage and public distrust, and regulatory compliance issues.

To address concerns surrounding legal liability issues, CISA provided provisions on legal liability and outlined the establishment of an ISAO for health care; the ISAO was in the initial stages of formalizing during the development and production of this report. However, many organizations still have concerns about sharing sensitive attack and incident data that they are not legally required to share because disclosure of that information could still harm the organization. This issue is not one that is unique to the health care industry, but likely has a greater impact due to the level of concern sector-wide about increasing regulatory authorities.

With the increasing emergence of fusion centers[24] and automated communications mechanisms, the increased volume of information shared creates an additional challenge as individuals can experience information overload, organizations must devote personnel to analyze the information, and personnel must be able to distinguish the relevant information from the "noise."

Strategy for HHS Communications with the Health Care Industry

Information sharing, communication, and establishing trusted relationships are critical components to protecting an organization's network and systems, preventing and identifying threats and potential attack vectors, and increasing situational awareness of what is occurring throughout the health care ecosystem. Communications with health care industry stakeholders can occur in a variety of divergent ways and should change over time to meet the current threat environment and needs of the community. However, to begin this industry-wide communication

[24] Fusion centers were designed to share information between Federal Agencies and at the State and local level government. Fusion centers collect information public and private sector sources.

and coordination effort, the HHS Secretary's primary focus should be on emphasizing and providing sector-wide education and training.

Communications can and should occur through both "push" and "pull" mechanisms; with the push mechanism HHS would proactively distribute information to the community and with the pull mechanism sector stakeholders would independently access the desired information. Push communications may include distribution of information through established portals, listservs and newsletters, and distribution of lessons learned from recent attacks. Pull communications may include website content and social media platforms, toolkits and trainings, stakeholder events, and webinars and podcast series. While some of the initiatives can be broad in nature and have a holistic focus across the sector (e.g., websites and social media content), many training and awareness activities (e.g., toolkits, podcasts) should be tailored to specific audiences to ensure the content provided is relevant, actionable, and timely. For example, the toolkit needed by a small hospital or regional provider to identify the current cyber threats and potential mitigations may be vastly different from the toolkit needed by insurance providers. Beginning with training and increasing awareness is the first step to reducing the probability of a successful attack and increasing the overall security posture not only of individual organization, but of the entire sector.

Presidential Policy Directive 21 and the National Infrastructure Protection Plan provide a mechanism by which industry sectors like health care can coordinate with the Federal Government on cybersecurity and other threats to the nation's infrastructure. These policies define 16 critical infrastructure sectors and establish a lead agency or agencies for each one. As the lead agency for the HPH Sector, HHS coordinates a partnership among private sector companies and trade associations representing the broad range of the health care industry with Federal, state, local, Tribal and Territorial agencies spanning operational, voluntary, and regulatory roles in the protection of cyber and other critical infrastructure. The HPH Sector Critical Infrastructure Partnership focuses on collaboration and information sharing, providing a common forum in which risks to health care organizations can be discussed and evaluated and collaborative risk mitigation activities can be developed. This partnership has more than a decade of experience navigating the challenges of information sharing and collaborative decision-making and can serve as a useful structure through which the health care industry and HHS can work to address cyber threats.

Note: Tie in recommendation of TF for cyber czar – HHS and how the 2 organizations would effectively work together.

VI Imperatives, Recommendations, and Action Items

Following nearly a year of discussions within the Task Force and information gathering from external stakeholders and subject matter experts across the health care and other sectors, the HCIC Task Force identified seven imperatives that must be accomplished collectively to help increase security within the health care industry. The Task Force-identified imperatives are:

- Develop the health care workforce necessary to prioritize cybersecurity awareness and technical capabilities.
- Enhance cybersecurity across the interconnected health care ecosystem.

- Increase the prevalence of and access to cybersecurity awareness and educational programs across health care industry stakeholders.
- Improve sharing and usage of cybersecurity information throughout the entire health care industry.
- Consider the unique challenges for health delivery organizations and small providers and develop incentives to increase overall cybersecurity posture.
- Increase the security and resilience of medical devices and health technology.
- Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.

Each imperative includes a set of recommendations and each recommendation contains one or more action items that define the concrete tasks that will assist in achieving the recommendation. Recommendations contained within the 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, it should be noted that coordination across the public and private sectors will be critical to accomplishing the goals. Each action item includes a proposed timeline in which the recommended entity should target to begin to address the action item. The Task Force determined based on funding required to complete the action, ease or difficulty of implementation, personnel resources available to complete the action, and effect on the overall security posture to the sector once completed. An action that includes a short-term timeline indicates the action should begin in [TIMEFRAME], medium-term indicates the action should begin in [TIMEFRAME], and long-term indicates the action should begin in [TIMEFRAME]. Once implemented, the imperatives, recommendations, and action items will help stakeholders across the sector and subsectors to increase awareness, manage threats, reduce risks and vulnerabilities, and implement protections not currently present across a majority of the sector.

It should be noted that while some recommendations are applicable to only certain health care subsectors, other recommendations (such as information sharing) are applicable to and valuable for the entire sector. While one could implement only a few of the recommendations and gain a minimal benefit, implementing the entirety of the recommendations contained in this section will compound the benefits to the overall security posture and program, as well as allow the organization to make the greatest use of financial investments and personnel resources.

Imperative 1. Develop the health care workforce necessary to prioritize cybersecurity awareness and technical capabilities.

Every sector faces challenges in meeting the workforce needs to recruit and retain qualified cybersecurity professionals. 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 moderate sized health care organizations, who 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 necessary to stay ahead of cyber threats.
- Limited resources with tight profit margins, particularly in the small and moderate sized organizations for re-investment into cybersecurity. Balancing the procurement of medical supplies (e.g. ambulance, x-ray machine) versus improved security technologies will continue to be a risk trade-off.
- Are we addressing the consumer in this report?

Commented [JC25]: Comment from Mark Jarrett: Think we need to emphasize that patients are both the victims of breaches and a portal of vulnerability

Recommendation 1.1: Develop a phased plan to get from the current, unsustainable state of workforce deficit to a desired end-state.

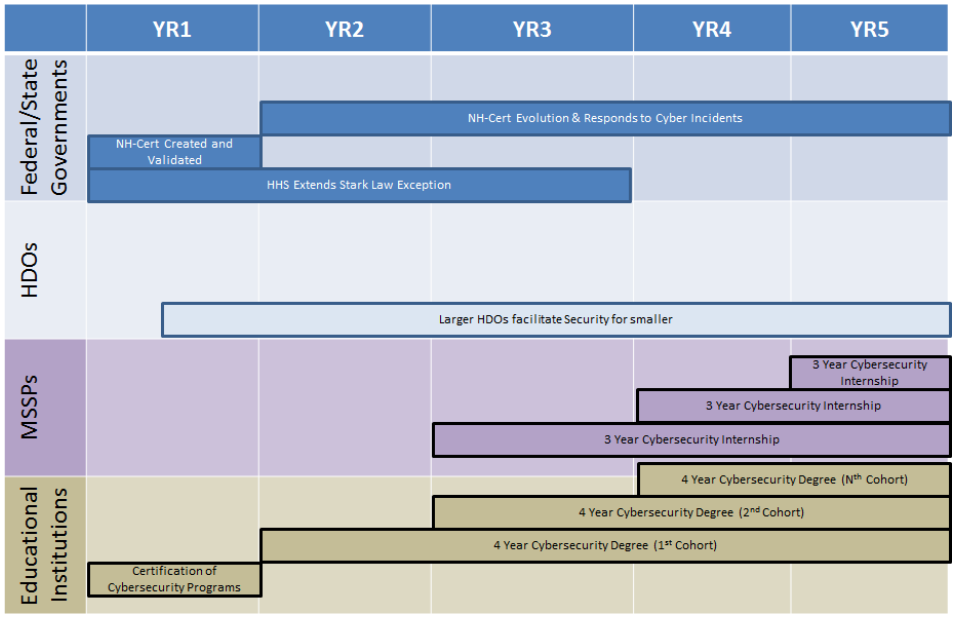
Independent of our constraints and opinions, there is objectively a minimum required talent pool and resources required to safely operate a modern, connected, health delivery organization. Many small, medium, and rural health care delivery organizations (HDO) have no qualified, dedicated security resources available to them. The prospect of supplying even one resource per HDO currently looks daunting, but is nonetheless necessary. California started the first safe patient ratio staffing system for Registered Nurses. This program evolved from a critical need to protect patients, nurses, and HDOs. We find ourselves in a similar situation regarding cybersecurity. There is a need for a similar ratio of health care cybersecurity expertise to the size of the organization. The larger the organization, the more security professionals are required. This ensures workload balancing across the organization to better protect the HDO, the clinicians, and most importantly the patients.

Commented [JC26]: Comment from Jacki: Does this really have to be the solution or this conclusive to that point? I continue to think that the small dental practice is never going to have a cyber security expert. I think we should tie in somewhere the ability for small practices to share resources in this space. Eg. today, I may have 1 info sec officer over 3 hospitals.

There currently does not exist enough properly credentialed and experienced cybersecurity professionals to fill this requirement. There must be a focus on developing a large and capable workforce while concurrently leveraging the current workforce and capabilities. The foundation of this proposal is the certification of educational programs. A simple search of the Internet yields hundreds of "cybersecurity" degrees across the Nation and around the world. While all valid degrees, the rigors and depth of knowledge varies from program to program. This Task Force recommends there be no more than three (3) bodies to validate and certify cybersecurity programs (e.g., Department of Homeland Security [DHS], National Security Agency, etc.). 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. To span this gap is a two-fold recommendation.

First, an exception to the Stark Law (CITE) for those larger HDOs which help smaller HDOs protect their systems, devices, and networks incentivizes increased security across the industry.

Second, the commercial managed security service providers (MSSP) organizations can develop a business and security model, essentially out-sourcing network security for smaller HDOs who have an operating budget to cover this cost. Both of these recommendations suggest the cybersecurity professional may not be on-site for all operations. To facilitate these models, it is recommended that a tiered cybersecurity workforce be considered. This model is already common within the health care setting (e.g., paramedic, nurse, nurse practitioner/physician's assistant, doctor). Focusing first at the biomedical engineer and IT staff, certify capable personnel to fundamental cybersecurity-related tasks (e.g., systems patching, asset inventory management, vulnerability management, etc.) within a yet-to-be-determined scope of practice. This approach ensures a "boots on ground" model to ensure basic functions and emergent responses are able to be addressed while leveraging the existing workforce.



Action Item 1.1.1: *Congress to provide financial support to no more than three accrediting bodies for cybersecurity education.*

Action Item 1.1.2: *Congress to direct the HHS Secretary to provide an exception to Stark Law to incentivize large HDOs to support small to medium sized HDOs. [Medium Term]*

Action Item 1.1.3: *Facilitate MSSP guidelines as documented in recommendation 1.2.*

Commented [JC27]: Comment from Jacki: What is the plan to cross reference items like this action with the longer Stark action I drafted on section 3?

Recommendation 1.2: Create a low-cost, MSSP model to support small and medium business health care providers.

Currently, the majority of small and medium business health care providers, clinicians, and rural hospitals face a significant struggle in hiring the appropriate level of IT human resources to support a "healthy" cybersecurity posture, as referenced in the manpower shortage section of this report. Individually these entities may not hold a large number of patient records; however, given a coordinated attack by nefarious actors on multiple small and medium business health care providers, the aggregated effect poses significant risk to national security. Breaches of small and medium business health care providers, both possible and realized, destabilize public trust in the health care industry at large and as such negatively impact the entire critical infrastructure sector. These entities are also an easy target for malicious users who intend on compromising patient records and systems.

We recommend the industry creation of a low-cost, MSSP model 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. Since these entities do not have the complex systems and networks or staffing necessary, the MSSPs should be able to standardize and develop an efficient and cost effective MSSP model. The low-cost 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. Additionally, these low-cost MSSPs provide a teaching and mentorship platform in order to grow the future cybersecurity professional workforce. Through Federally supported internships, emerging cybersecurity professionals gain essential work experience in the field.

Action Item 1.2.1: *Incentives and grants by the Government to encourage more number of low-cost MSSPs to support small and medium business health care providers. [Medium Term]*

Action Item 1.2.2: *Tax incentives by the Government to encourage health care providers who invest in security technologies and MSSPs. [Long Term]*

Action Item 1.2.3: *Regulatory agencies such as the Office for Civil Rights (OCR) should provide a reasonable credit to small and medium business health care providers who have engaged low-cost MSSPs during their audits and breach investigations.*

Action Item 1.2.4: *The low-cost MSSPs could also provide Information Security Officer level support for these small and medium business health care providers.*

Action Item 1.2.5: *Information sharing and exchange of vulnerabilities and threat information between Information Sharing and Analysis Center [ISAC] and/or ISAOs (i.e., National Health Information Sharing and Analysis Center [NH-ISAC], Health Information Trust Alliance [HITRUST], etc.) and low-cost MSSPs who support small and medium business health care providers.*

Action Item 1.2.6: *The low-cost MSSPs should institute ongoing internship programs to develop more information security professionals in supporting the health care industry.*

Commented [JC28]: Comment from Mark Jarrett: This should coordinate or combine with "shortage of security expertise" section. Also, on amending the Stark law

Commented [JC29]: Comment from Jacki: This will benefit a really small portion of the sector and not likely most of the healthcare provider space who are tax exempt.

Recommendation 1.3: Develop efforts to increase cyber-literacy across divergent members of the health care industry.

The provider community in the U.S. quickly adopted EHRs driven by two forces: 1) the recognition of the value of information sharing to promote quality and safe care, and 2) the ability to offset some costs using Meaningful Use dollars. Unfortunately, with this rapid spread a process was not created to educate providers on the cyber risks in their new environment. This applies to both clinicians such as physicians, nurses, etc., as well as to administrators of hospitals and free-standing ambulatory sites. Although large hospitals and health systems have the resources and experience to address cybersecurity, much of the health care community does not. Vulnerability exists because most people are unaware of the risks and also do not have the tools to protect their systems. This is true even in their personal lives. A national education program designed specifically for non-technologically sophisticated health care users can fill this gap. 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, one for administrators, and one for non-provider daily users, such as registrars. Also, a pre-course survey would help provide information to define the knowledge gap so the program can be constantly updated.

Action Item 1.3.1: *ONC should develop a national health care cyber-literacy course. There will need to be biannual updates for this rapidly changing environment.*

Commented [JC30]: Comment from Jacki: We may want to highlight or at least acknowledge that there was some security requirements for the acknowledgment process.

Commented [JC31]: Comment from David Ting: There could be arguments that providers, especially those in hospitals, have been educated on security risks associated with HIPAA and MU1 requirements so a broad statement like this will likely be challenged.

Commented [JC32]: Change to HHS? ONC does not have the budget or staff to do this.

Recommendation 1.4: Develop cyber safety best practices.

Need to change the culture of health care organizations that cybersecurity is an IT problem. Cybersecurity is everyone's responsibility, from buying and implementing secure products to ensuring the use and behavior of users do not put the organization at risk. Clarify that cybersecurity protections and mission goals are not conflicting objectives. Recognizing that the risk across an organization and cyber protections will vary based on mission needs from emergency rooms to patient intake.

Action Item 1.4.1: *Resource an ongoing education campaign addressing both end-users and Chief Executive Officers/boardroom.*

Action Item 1.4.2: *Establish a code of conduct so consumers know how they can effectively share health care information with their providers in a secure manner.*

Action Item 1.4.3: *Ensure Internet of Things vendors provide clear information on how they will use/share consumer information.*

Commented [JC33]: Comment from David Ting: Do end-users refer to clinicians or patients or both?

Commented [JC34]: Comment from David Ting: We use the term consumers and patients interchangeably – need to be consistent on the meaning.

Commented [JC35]: Comment from David Ting: Lots of issues around data generated by patient IOT devices - everything from data privacy, security, patient ID, etc. this action seems to cover a lot.

Recommendation 1.5: Workforce and resources not available for even current connectivity.

The technology adoption by health care organization has outpaced the technical capabilities of many organizations with tight financial resources and limited IT workforce. These resource and workforce gaps needs to be addressed with interim solutions while long-term plans are established within the sector. Existing technologies in place should continue to be secured and protected. Although not a replacement for building more secure products or comprehensive

Commented [JC36]: Comment from David Ting: Not sure what we mean by outpaced? Some will argue the successful adoption of EHRs to meet MU1 demonstrated technology adoption so we need to be clear what we mean.

cyber risk management strategies, the existing capabilities can help to help highlight the highest risk elements that could be more effectively secured today.

Action Item 1.5.1: *Partner with industry to establish low-cost/impact self-assessments for non-IT staff to evaluate potential risks of existing organization IT.*

Action Item 1.5.2: *Fund Federal or private teams which could be deployed to assess organizations and provide timely recommendations to adopt secure solutions. NOTE: Need to address the liability risks of helping/recommendations.*

Action Item 1.5.3: *Develop a health care mentoring program to help educate non-IT staff to proper risk management of IT and information sharing.*

Recommendation 1.6: Identify and designate a CISO/security leader who will have responsibility for and authority over the organization's information and cybersecurity policies, processes, and functions.

Most health care organizations today would benefit from sufficient resources to help ensure that cybersecurity requirements are fulfilled and maintained. Such resources would address business needs as well as regulatory mandates. In order to provide effective leadership over the cybersecurity/information security function, health care organizations should designate a CISO or other officially designated individual that serves as the most senior cybersecurity/information security professional. At a minimum, this individual should be responsible for ensuring appropriate corporate security policies are established and enforced.

For some health care organizations, it may not be feasible to have a team of resources dedicated exclusively or primarily for cybersecurity matters. However, it is important that such organizations designate a specific individual to provide leadership and make decisions pertaining to cybersecurity initiatives and issues. This individual must have both the official authority, as well as the appropriate expertise to carry out such responsibilities. Ideally, this individual will be assigned the CISO/security leader as their exclusive role and area of responsibilities. For some organizations, a full-time dedicated resource for this role may not be feasible; in such instances, an individual should be assigned the CISO/security leader role as an official component of a broader role. 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 1.6.1: *A mandate for health care organizations should be established that strongly encourages the designation of a CISO or official security leader.*

Recommendation 1.7: Small and medium-sized health care providers should migrate patient records and legacy systems to secure cloud service providers.

Small and medium sized health care providers continue to maintain local servers and databases with their patient data even though many providers have started using cloud-based EHR vendors. A majority of these providers still have legacy EHR systems, aging infrastructure, and capital investment limitations. This segment of providers has not been able to cope up with the

Commented [JC37]: Comment from Mark Jarrett/Theresa Meadows: This doesn't seem practical

Commented [JC38]: Comment from David Ting: It seems like we talk about the lack of CS professionals and then we recommend having a CISO for every organization. Just concerned this recommendation is not consistent with what was said earlier

Commented [JC39]: Comment from Christine Sublett: It would be appropriate to utilize a part time, external resource for small healthcare and health tech organizations.

Commented [JC40]: Comment from Mark Jarrett: How does this work in a two physician practice? Perhaps we propose for these small sites a security leader who cover s a region's small practices?

Commented [JC41]: Comment from Jacki: I wonder if we should include that they could leverage a consultant for this purpose vs. needing an internal individual.

Commented [JC42]: Comment from Theresa: I need to understand this recommendation more. I don't think we should recommend how people store and protect their data. As a large provider, I am not sure we would do this so I want to make sure we are all in agreement with this recommendation. The reason I would not put this is a recommendation is not the security aspect but all the other operational issues that can occur with Cloud Service providers.

Commented [JC43]: Comment from Mark Jarrett: They will need a back-up site as well – this needs to be considered – for business continuity.

Commented [JC44]: Comment from David Ting: Not sure if we all agreed this migration to a cloud service provider is the right or only approach. There are lots of hosting services (EPIC, Cerner, etc) that can provide secure EHRs – a recommendation to move systems to the cloud seems to be an oversimplification

technology advancements due to their limited IT support and security resources. As such, we recommend these providers to consider migrating their patient records and legacy systems to secure cloud service providers with disaster recovery capabilities.

Cloud service providers have made significant advancements in security controls and technologies. In fact, some major cloud service providers have already started offering HIPAA-compliant secure cloud computing environments. As these cloud service providers operate on a low-cost, pay-as-you-go model, the small and medium business health care providers may likely spend less money on the maintenance of legacy systems. By moving to a secure cloud environment, health care providers will have a peace of mind and effectively use their clinical resources to support their patients without having to worry about maintaining their on-premise infrastructure and systems.

Action Item 1.7.1: *Incentives and grants by the Government to encourage more number of Secure Cloud Service Providers to support small and medium business health care providers.*

Action Item 1.7.2: *Tax incentives by the Government to encourage health care providers migrate to a secure cloud environment. [Long Term]*

Action Item 1.7.3: *Regulatory agencies should provide more guidance to HIPAA-compliant cloud environments and create more awareness among health care providers.*

Action Item 1.7.4: *Major Cloud Service Providers should develop cost-efficient partners and support organizations to easily on-board small and medium health care service providers.*

Action Item 1.7.5: *Insurance companies should provide more incentives to small and medium health care service providers who migrate to a secure cloud environment.*

Recommendation 1.8: Workforce 'barriers' a) STARK prevents 'sheriffs'; b) no $'s for CISO @ sm/med/rural; c) no pool of CISOs to hire @ sm/med/rural

An underlying problem for cybersecurity in health care is the huge disparity in resources among hospitals and outpatient providers. In addition, there is a national shortage of experts in cybersecurity. A more practical approach would be for smaller providers to employ IT staff (which in a small critical access hospital might be only one IT person) who has extra training in cybersecurity. This resource(s) will need back-up, but unrelated entities cannot offer free or nominal cost back up as this might be considered inurement according to Stark regulations. HHS should explore ways in which the Secretary of HHS may be able to use existing authorities to overcome these barriers. This would facilitate those with more resources being able to support other non-affiliated entities in their community.

Action Item 1.8.1: *Secretary of HHS declares information sharing and support of cybersecurity between non-affiliated health care entities a Stark exception. [Medium Term]*

Recommendation 1.9: HITECH money for rural connect EHR. (incentive for industry low cost MSSP).

Commented [JC45]: Comment from Theresa: Can we discuss this at the February meeting? Not sure I agree with this recommendation. I would prefer to take out the cloud reference and encourage incentives to implement technology period. Should not be only cloud.

Comment from Lauren Thompson: This is essentially recommending a technical solution. Is this appropriate?

Commented [JC46]: Comment from Jacki: HIPAA is the floor in my opinion related to security so do we really want to say that if it's HIPAA compliant we aren't going to have cyber issues? I think this is a risky statement

Commented [JC47]: Comment from David Ting: These generally are for clinics and ambulatory clinics rather than hospitals. Cloud use introduce other issues that we haven't discussed.

Commented [JC48]: To be merged with recommendation 1.1

Commented [JC49]: Comment from David Ting: Increasingly larger HDOs with EPIC or Cerner are offering EHR access to their affiliated clinics and practices to both support better patient care and to eliminate the need for the practices to manage their own IT solution (and cybersecurity).

INSERT TEXT

Action Item 1.9.1: *TEXT*

Imperative 2. Enhance cybersecurity across the interconnected health care ecosystem.

INSERT TEXT DESCRIBING THE IMPERATIVE

Recommendation 2.1: Framework

The health care industry in the United States is a mosaic, consisting of 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. Great strides have been made over the last ten years in connecting the many stakeholders utilizing information technology to improve health outcomes and create value. This vast electronic network, however, needs to ensure privacy and security for all users, especially patients. This vulnerability for health care information has become very evident in the last few years with identity theft, ransomware, and targeted nation-state hacking becoming more frequent and extensive. To achieve the goal of cybersecurity in the health care environment, a framework for improving critical infrastructure cybersecurity needs to developed and implemented for this industry. Although National Institute of Standards and Technology (NIST) has developed a generic framework, health care 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, the latter essential for good patient care. The framework will promote a single lexicon for health care as well as standards, guidelines and best practices. The complex environment will require certain basic standards that all must meet and guidelines that allow flexibility for select issues. Without this roadmap, any of the countless constituents may pose a risk to the system.

Action Item 2.1.1: *NIST and ONC: develop a custom framework built on the NIST general framework that accommodates the unique issues of health information technology intersecting with cybersecurity. [Short Term]*

Commented [JC50]: Comment from Jacki: This seems repetitive of what's above. I am not sure I get what we are trying to say here that's different from above. I recommend consolidating or making it more clear as to how its different from above.

Commented [JC51]: Comment from Thad/OCIO: OCIO is kicking off an effort, in partnership with ASPR, ONC and other OpDivs as well as the HPH SCC to support this activity.

Recommendation 2.2: Congress should require Federal regulatory agencies to harmonize existing and future laws and regulations that affect cybersecurity.

The health care industry faces significant challenges due to State and Federal cybersecurity laws and regulations that are inconsistent and establish different standards of compliance. To understand 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;
- Spyware laws in 20 States and two territories; and
- Phishing laws in 23 States and one territory.

These laws work in conjunction with laws on data breach notification, data disposal, and data security, often dictating different responses than Federal laws such as HIPAA. 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 are often required to follow the regulatory and legal requirements in order to meet the patchwork of standards, rather than utilizing technology and cybersecurity practices that truly protect patients. The top priorities for regulatory agencies should be to ensure consistency among various State and Federal laws so 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 statutory and regulatory inconsistencies.

Further exacerbating the quagmire of State and Federal laws, some regulatory agencies have a strict liability standard in their evaluation of incidents. This means that even when the organization is making a reasonable and good faith effort to comply, it may still receive a regulatory fine or penalty, or be sued for damages. This creates many challenges for organizations with limited resources. The health care ecosystem should be focused on a cybersecurity framework that includes risk management evaluation with the priority being keeping patients and their information safe – not complying with costly baseline and often conflicting regulations. Because compliance with laws and regulations will supersede any investment in cybersecurity that may actually help protect the patient, the health care ecosystem does not have the financial means to focus on keeping patients as safe as possible. We recommend that the focus should be on the harmonization of existing and future laws to remove the resource and financial burdens, such as those created by strict liability laws, and allow organizations to implement cybersecurity frameworks that will keep patients as safe as possible.

Action Item 2.2.1: *Establish a task force to make recommendations for harmonization.*

Recommendation 2.3: Require strong authentication to improve identity and access management in accordance with recommendation 1.3 in the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital Economy*.

Commented [JC52]: Comment from Lauren Thompson: Suggest we try to streamline to be more concise to align with other recommendations

Health care IT services present unique cybersecurity challenges. The delivery of health care is premised on the establishment of a trust relationship between and among providers, patients, and medical devices. The foundation of this trust is the belief and confidence in the identities of the individuals involved (providers and patients) and their right to engage with medical devices in the course of treatment. Any threat to the trust relationship can, at a minimum, delay the delivery of care and has the potential to cause severe injury or death. We believe 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 the means for accessing clinical information systems, will allow providers and patients to maintain this trust relationship for the foreseeable future.

The use of strong authentication to improve identity management in the delivery of health care will help ensure security and privacy in a manner consistent with Recommendation 1.3 of the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital Economy*.

Health Care Workers: Health care workers access information in a manner quite different from workers in the traditional knowledge economy. Whereas most of us log on to a single computer no more than several times a day, clinicians in a hospital setting are required to access multiple

computers throughout the facility over and over again, 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 cyberattack, as such passwords can be weak, can be stolen, and are vulnerable to external phishing attacks, malware and social engineering threats.

An alternative to the use of passwords for user authentication has been adopted by the NIST in its electronic authentication guideline Special Publication (SP) 800-63. Whereas a password is something that is known and memorized by a user, the NIST-approved solutions for user authentication include (i) items that are in the user's possession, like a proximity card or a token and (ii) items which are unique to the individual, such a biometric modality like a fingerprint, a palm print or an iris. The Drug Enforcement Administration has implemented regulations based on the NIST standard for the electronic prescribing of controlled substances (EPCS) and these are used by several States that have adopted EPCS requirements. By replacing traditional passwords with one or more of these alternatives, the health care industry can significantly reduce the risk of cyber theft while at the same time increasing productivity. Studies have shown that providers typically see time savings from around 20-30 minutes to as high as 45 minutes per clinician per shift when passwords are replaced with token or biometric user authentication.

Patients: Just as the need to authenticate providers is critical to the establishment of the trust relationship in the delivery of health care, so it is becoming more important that patients accessing electronic information be properly identified and authenticated, too. Patient access to health care services requires the same level of confidence in establishing rights to access or modify medical records, to schedule appointments, as well as to receive care. The U.S. Government introduced the "Meaningful Use" program as part of the 2009 *Health Information Technology for Economic and Clinical Health Act.* Among other things, Meaningful Use requires health care providers to show the use of EHR systems by patients, and includes financial incentives for showing patient access of such systems. Similar to the challenges outlined above for providers, the use of passwords as the means for patient access to electronic medical records introduces cybersecurity vulnerability. Passwords can be can be forgotten, misplaced, and stolen by cyber criminals; patients are particularly vulnerable to such schemes as phishing scams and malware introduction. In order to participate in digital transformation of health care from a traditional "brick and mortar" experience to an increasingly online experience, multi-factor authentication leveraging biometrics, mobile phones or wearables are required to establish a trust relation. Most of us are already familiar with such policies as we access financial records. Similar mandates should be implemented for patients seeking to access their medical records.

Medical Devices: The same trust relationship that exists between provider and patient must include medical devices as well. In our modern world, these devices play an increasingly common role in the provision of health care. IV infusion pumps deliver prescribed dosages of medication; nuclear magnetic resonance (NMR-CT) imaging machines expose patients to radiation as they scan the anatomy; and robotic radio surgery is used to perform precise incisions. The integrity of the devices used in these treatments, and other similar technologies, must be assured from a bioengineering and a cybersecurity perspective in manner no less than used to protect the privacy of medical records. The provider operating the device must be authenticated and be authorized to operate it, and the patient needs to be accurately identified as

the person authorized to receive the treatment. To accomplish this, multi-factor authentication modalities, similar to those referenced above, can be utilized. For example, providers can be required to use a token or a biometric identifier to operate the machine. Similarly, a patient can utilize a biometric (palm, fingerprint or iris), mobile phones, or wearable token to verify their identity as the individual authorized to receive treatment.

Action Item 2.3.1: *We strongly urge the Commission to adopt the recommendations contained herein to ensure that the trust relationship between provider, patient, and medical device that is the foundation of the delivery of health care services in the United States is maintained and enhanced in the digital age.*

Action Item 2.3.2: *In situations where the provider is accessing an EHR or HIE external to the hospital or clinical, we recommend the Commission adopt the NIST SP800-46 guidelines for remote access including the use of two factor authentication to ensure a compromised password cannot alone be use to gain access.*

Recommendation 2.4: The Federal Government and the health care industry should work together to establish standard approaches and structures for cybersecurity governance and accountability at and within health care organizations (both covered entities and business associates) and organizations working with health care organizations.

While Federal regulation calls for designated privacy and security officers in covered entities, this has neither been done 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).[25] This disparity in accountability and responsibility complicate and delay 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. This disparity across a sector that comprises roughly 17 percent of our gross domestic product is unmanageable and unsustainable if health care is to be delivered timely, efficiently, and in cost effective ways while protecting the security of our organizations and the privacy of our patients.

Action Item 2.4.1: *The Federal Government in coordination with the industry should develop industry-led, consensus-based governance models for cybersecurity that support a variety of health care organizations from large integrated care delivery systems to small physician practices, public and private, not-for-profit and for-profit.*

These models should also be applicable the wide range of business associates in the sector. Governance is an issue of responsibility and authority not specific cyber expertise and management of these organizations must be engaged in security from identifying assets, risks, and governance to protection planning including controls, training, processes and procedures, and technology to response planning and communication and ultimately recovery from cyber

[25] McGraw, D., Ingargiola, S., Wallis, K. *Business Associate Compliance With HIPAA*. Retrieved from: https://www.manatt.com/getattachment/0b19cc2d-ed14-458b-a4bc-7b4436437c4f/attachment.aspx

events. Many organizations in other sectors have begun to include cybersecurity experts on their Boards of Directors. This should be encouraged in health care.

Action Item 2.4.2: *The sector should be required to use the NIST Cybersecurity Framework. [Short Term]*

This should not preclude any business from using a framework of their choice or design internally but when working with other organizations in the health care industry this will speed and enhance communications in regard to risk, cybersecurity and management of those areas, and driving the historic compliance approach toward a more holistic cybersecurity risk management approach. It will also expedite cybersecurity information sharing across all critical infrastructure sectors.

Action Item 2.4.3: *Recognizing that not every organization will be able to find, hire, and retain cybersecurity expertise, the Federal Government should establish minimal standards for security that can be implemented without creating long-term staffing needs on the part of the health care organization.*

This means that the broad, descriptive measures of the HIPAA security rule will have to have firm "floors" and clear prescriptive minimum requirements (e.g., password requirements, defined backup procedures, definite disaster recovery plans).

Action Item 2.4.4: *Regulatory agencies involved in the health care industry should harmonize existing and future regulations with the NIST Cybersecurity Framework to focus on risk management. [Short Term]*

This will reduce the industry's cost of complying with conflicting regulations that may not aid cybersecurity and even unintentionally discourage interoperability.

Recommendation 2.5: Combine the practices outlined in the ONC SAFER guide with those described in the NIST Cybersecurity Framework.

Health care today is based on having accurate medical information for patients so clinicians can make timely decisions about care. The transition from paper records has resulted in accelerating the speed and ease with which information can be accessed, modified, and delivered to providers. This transformation has tremendous potential for improving quality and patient safety. However, these same benefits also increase the susceptibility of the medical records to unintentional or deliberate manipulation of the data that can lead to compromised patient care, care coordination, and quality reporting and research as well as fraud and abuse.[26] A lack of trust in the integrity of medical records within an EHR can result in a denial of service like attack when providers cannot rely on the information for their decision making and be forced to either revert to older records or re-verifying patient lab results.

The ONC sponsored SAFER guides (Safety Assurance factors for EHR resilience) focused on six basic tenets of safe and effective EHR implementation and use, stating that "EHRs must be:

Commented [JC53]: Do we want to say required, or recommended/encouraged?

Commented [JC54]: Comment from Christine Sublett: Tied to NIST Standards?

Commented [JC55]: Comment from Vito: Somewhat redundant with what was addressed under Imperative 1 and Workforce. Maybe this action item can be added Imperative 1 action items.

[26] AHIMA. (2013). *Integrity of the Healthcare Record: Best Practices for EHR Documentation*. Retrieved from: http://library.ahima.org/doc?oid=300257#.WG_m-lUrKw4

- Available when and where they are needed
- Only viewed by authorized users
- Only modified by authorized users
- Used correctly and completely throughout the organization
- Must be designed and implemented to promote safe, effective and efficient use
- Must have mechanisms in place to monitor, detect and report on the safety of the EHR"[27]

HIPAA compliance addresses the privacy issues for medical records but does not address the issues around documentation accuracy which encompasses governance, patient identification, authorship validation, amendments and record corrections – all critical to providing EHR resilience.

Action Item 2.5.1: *ONC should combine the practices outlined in the SAFER guide*[28] *with those described in the NIST Cybersecurity Framework. The SAFER offer practical self-assessment guides specific to EHR deployment to ensure resiliency for the EHR system. Many of these overlap with the NIST Cybersecurity Framework's main categories of identify, defend, detect, respond, and recover but are more clinically relevant.*

Recommendation 2.6: The Federal Government should create a cybersecurity leader role within HHS to align and coordinate internal and external portfolios.

CISA requires HHS to provide "…a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity in the health care industry…" This is important because there are currently many different programs and agencies within and outside HHS with responsibility 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 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.
- Promotes efficient decision-making during normal operations as well as response to cyber incidents.
- Enables HHS to advocate more effectively for health care cybersecurity as a whole.
- Allows HHS to leverage cyber expertise from multiple programs, including those with regulatory responsibilities, those with non-regulatory cybersecurity roles, and those who are responsible for HHS's internal cybersecurity operations.

[27] Sittig, D., Ash, J., Singh, H. (2014, April). *ONC Issues Guides for SAFER EHRs*. Retrieved from: http://library.ahima.org/doc?oid=300417#.WHUnLP_rsuR
[28] HealthIT.gov. *ONC's SAFER Guides*. Retrieved from: https://www.healthit.gov/safer/safer-guides

While naming one individual will be very helpful in addressing the above issues, one person alone will not be able to address all of the needs of the health care industry with respect to cybersecurity. It is recommended that in addition to naming the individual HHS also develop and communicate:

- HHS's structure for addressing cybersecurity, including program names, areas of responsibility, and points of contact.
- A single website that can serve as a "one stop shop" for linking to HHS's various cybersecurity programs and resources.
- The mechanism by which health care industry partners can collaborate with HHS on an ongoing, voluntary basis to address cyber risks.

The creation of this cyber leader role at HHS would mark a critically important step in elevating the security posture of health organizations across the nation. With this new role, the health care industry can lead by example and leverage the capabilities and outreach of OCR, ONC, and ASPR to help the sector improve its preparedness for and response to security incidents now and into the future. HHS's cyber leader should align and coordinate internal stakeholders to collaborate with the private sector, NIST, and DHS to develop voluntary guidelines to support adoption of the NIST Cybersecurity Framework, and support health care industry risk reduction and resilience.

Commented [JC56]: Per Emery: How does the task force see this role with other roles – FDA, CMS, NIH? Or are you specifically recommending only for OCR, ONC and ASPR.

Comment from Theresa: I absolutely believe the FDA and CMS must be included in this outreach.

In order to optimize the effectiveness and efficiency of this role the Task Force believes, given current organization structure, the position should report to the HHS Deputy Secretary, who has overall leadership within the Department for cybersecurity and chairs the HHS Cybersecurity Working Group. The HHS Cybersecurity Working Group is the principal forum for drive coordinating across HHS operational divisions and components, to better align resources, communications, and support to external stakeholders across the Federal sector, State and local governments, ISACs and ISAOs, and the health care industry.

Through the HHS Cybersecurity Working Group, the cyber leader can support increased information sharing, risk management, and resilience within the health care industry, through: coordination the Department's internal and external communications, awareness, engagement, and support to the health care industry, as well as supporting the alignment and promotion of resources to support cybersecurity risk management, awareness, information sharing, and incident response.

Action Item 2.6.1: *This cybersecurity leader should be tasked with creating a sector-specific plan to establish goals and priorities for cybersecurity. These would include but are not limited to the following:*

(1) Ensuring adequate threat response and a plan of action for such effective response, such as through the use of a universal framework for information cybersecurity and privacy;

(2) Encompassing holistic security and what that would entail for the sector (including software manufacturers, medical device manufacturers, health care providers, health plans, and others);

(3) Fostering interdependence between the health care industry and other identified critical infrastructure sectors;

(4) Expanding the pool of qualified cybersecurity personnel;

Commented [JC57]: How, considering they are already in short supply in existing sectors? Who defines "qualified"? Maybe by expanding HEAL program and requiring work within provider sector for a period?

(5) Advancing workforce education on privacy and security awareness at health-related organizations and a plan of action to enable the same, such as through the widespread dissemination of key messages and new threats prominently displayed in common areas (e.g., break-rooms);

(6) Incorporating lessons learned from Regional Extension Centers and other successful programs to advance greater outreach to small providers;

(7) Advancing bidirectional, timely cyber threat information sharing between the Federal government and health care industry stakeholders. This could be through existing structures like the National Cybersecurity and Communications Integration Center (NCCIC) and others such as the NH-ISAC, as well as less technical communications that still provide actionable information on threats, vulnerabilities and risks to organizations less able to ingest and process highly technical data such as indicators of compromise; and

(8) Advancing the state of health IT and creating a plan of action to ensure that it is created, operated and maintained with privacy and security in mind.

Action Item 2.6.2: *This cybersecurity leader would be tied directly to other Federal Agencies tasked with cybersecurity such as DHS, the Federal Bureau of Investigation (FBI), and others.*

Commented [JC58]: Comment from Lauren Thompson: What do we mean by "tied directly"?

Tying these Federal entities to the cyber leader would help to assure coordinated plans, responses, approaches, and strategies to cybersecurity across all sectors of U.S. Government and business and industry sectors.

Action Item 2.6.3: *The action steps outlined in the health care industry specific plan should be used by stakeholders to create, adopt, and implement robust cybersecurity solutions.*

By engaging the entire community to build and deliver cybersecurity capabilities, security is enhanced across the sector and for the Nation.

Recommendation 2.7: Congress should pass an amendment to the Stark Law to allow an exception for health care providers seeking to donate or subsidize cybersecurity programs to physicians and their practices.

Commented [JC59]: Used to be recommendation 5.2

Comment from Aftin: Since the other recommendations in this section have been absorbed by imperative 6 which is focused on medical devices, for now I am suggesting putting this in section 2 which is a catch all for different ideas to see how this groups with other recommendation areas

The Stark Law governs physician self-referral for Medicare and Medicaid patients. Under the Stark Law, a physician is prohibited from making a referral to an entity for the furnishing of designated health services payable by Medicare or Medicaid if the physician, or an immediate family member of the physician, has a financial relationship with the entity, unless an exception applies. Although Stark serves as a stringent barrier to protect against fraud and abuse among health care providers, the law often proves inflexible in the context of rapidly advancing health care technology. Donating cybersecurity products and services to physicians and their practices would help protect the safety of patients, particularly in regard their clinical care, in the broader health care ecosystem due to interconnectivity among health care providers.

Similar to the exception created for donating EHRs, we strongly encourage Congress to pass an amendment to the Stark Law specifically for cybersecurity software that would allow health care organizations the ability to assist physicians in the acquisition of this technology, either through donation or subsidy. The Stark EHR exception 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 software without trained security professionals who have the expertise to provide sufficient cybersecurity programs to protect their patient records. We need to empower physician practices to actively manage their security posture, not hinder them. Often organizations want to assist these providers by providing technology and expertise that will be mutually beneficial to protecting patients and their information, but are not able to achieve this desire with the constraints from the Stark Law. An exemption will provide for this assistance without creating fear of violating the Stark Law.

Action Item 2.7.1: *Congress should create an exemption to the Stark Law for cybersecurity to allow organizations to assist physicians with education and technology on the subject matter.*

Recommendation 2.8: Insurance role; cyber

The insurance market for cybersecurity is evolving. HHS leadership should partner more closely with DHS in helping identify a roadmap to enable private industry development 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.

Commented [JC60]: Comment from Jacki: Not sure what this means? I thought this possibly had to do with cyber insurance holding the industry to a higher standard when evaluating for premiums or doing rate credit for those they have good programs? I think Marsh brought it up.

Action Item 2.8.1: *Integrate with DHS efforts to support the development of insurance marketplace in support of the health care industry.*

Action Item 2.8.2: *Identify integrated models for reducing potential costs/risks associated with insurance through the adoption of MSSP for small/moderate sized organizations.*

Action Item 2.8.3: *Liability Safe Harbors? TBD.*

Recommendation 2.9: Supply Chain

Approximately 600,000 people work supporting the medical supply chain in the U.S. This does not include products from outside the U.S. The mix of traditional and health care specific technologies continually introduces new risks to organizations. Each product has a supply chain of providers and integrators that contribute to the overall risk posture.

Commented [JC61]: Comment from Mark Jarrett: Did we ever discuss foreign product vulnerabilities anywhere????

Action Item 2.9.1: *Incentivize the development and adoption of secure operating systems for medical devices and the Internet of Things.*

Action Item 2.9.2: *Model for collecting/reporting vulnerabilities across supply chain/bill of materials.*

Action Item 2.9.3: *Incentivize the replacement of legacy technology with newer secure alternatives. Consumer reports like rating of IT when making selections.*

Recommendation 2.10: Enhancing cybersecurity across interconnected health care ecosystem

Innovation in industry has demonstrated several methods, which have proven successful and should be encouraged within the health care industry to enhance security across the health care ecosystem. However, the regulated environment in health care may delay adoption of new approaches while a "wait and see" approach is taken to risk failure. With the momentum of the Internet of Things and new technology, a more aggressive approach needs to be encouraged by HHS to explore and incentivize.

Action Item 2.10.1: *Encourage adoption of MSSPs to ensure a foundation of secure capabilities.*

Action Item 2.10.2: *Develop profiles within Cybersecurity Framework that organizations can use when evaluating partnerships risks for sharing information.*

Action Item 2.10.3: *Encourage the adoption of secure APIs?*

Action Item 2.10.4: *Further research in the use of block chain in health care (Fred/FDA)*

Commented [JC62]: Comment from David Ting: Feels like we are making specific technology choices

Commented [JC63]: Comment from Theresa: I need more information on these two items

Recommendation 2.11: The private sector should develop conformity assessment programs in accordance with action item 1.4.4 of the Commission on Enhancing National Cybersecurity's Report on *Securing and Growing the Digital Economy.*

Hospitals and long-term care facilities are obligated to adhere to Joint Commission standards and CMS conditions of participation. Physicians in non-hospital employed practices (still the majority), however, are not subject to the rules of those accrediting bodies. Also, these practices employ clinical and non-clinical staff that receives variable levels of training as well as having a wide range of educational backgrounds. Therefore, a solution is needed that encompasses all providers and their staff in addition to the above mentioned regulated provider sites. Although the OCR has started to look at accreditation, this approach should be reconsidered. Utilizing an agency that has a significant punitive arm may result in providers "checking the box" for compliance but not really engaging in the process. A neutral body, such as ONC, should set a standard (based on criteria referred to in other sections of this report). Enforcement could not be tied to licensure of the providers as this is a State function, nor to payment as not all providers participate in Medicare or Medicaid. A better alternative would be that a requirement for linking to any health information exchange, laboratory, or other information-sharing platform would require this accreditation. Inability to link to other systems would be a barrier that will make non-accreditation an unacceptable alternative. To make this a robust program there needs to be developed an audit process that randomly checks compliance.

Commented [JC64]: Comment from Jacki: This isn't accurate for all organizations. One could be accredited by their own state department, CMS or Joint Commission amount other possibilities.

Commented [JC65]: How would a small provider do this?

Action Item 2.11.1: *ONC should develop an accreditation process for cybersecurity health that all providers must obtain in order to be on any health information exchange.*

Recommendation 2.12: Create a strong audit awareness program and ongoing cybersecurity audits to understand the challenges and gaps within the health care industry.

The HIPAA compliance program has been in place since 2003. However, the adoption and the compliance levels have been less than satisfactory. Recent OCR audits and cybersecurity breaches continue to reveal that the health care industry (especially health care providers) has not addressed even the minimum security requirements outlined in the HIPAA compliance program. A majority of small and medium-sized health care providers still do not have a sufficient level of education and awareness regarding HIPAA compliance and the importance of protecting their patient records. A majority of these small and medium business health care providers continue to experience security incidents and breaches. However, these providers do not have the right level of resources to detect, monitor, and investigate these incidents and breaches. On the other hand, regulatory agencies like OCR have not conducted a sufficient level of audits across these small and medium business health care providers to create a strong cybersecurity and compliance momentum across the industry. Unlike the banking and financial industry, the patient records may be present at a small dentist, urgent care facility, and also a large health care system. The regulatory agencies including HHS, OCR, FDA, and the Joint Commission have to determine how they can create a strong awareness and ongoing audits to understand the challenges and gaps within the industry.

Action Item 2.12.1: *OCR should partner with security auditing and consulting firms to conduct increased audits and monitoring across small and medium business health care providers and vendors to identify specific challenges across different subsectors.*

Action Item 2.12.2: *OCR should review their existing HIPAA compliance requirements and develop additional requirements, such as ongoing security monitoring and focus on cyber hygiene of health care systems.*

Action Item 2.12.3: *OCR should develop guidance documents to capture specific risks and best practices for different subsectors such as dental practices, physician practices, urgent care programs, and vendors.*

Action Item 2.12.4: *HHS should consider offering incentives for security companies who provide security support to small and medium business health care providers.*

Action Item 2.12.5: *Regulatory agencies and accreditation bodies (i.e., OCR and FDA) will have to create stronger cybersecurity enforcement programs among health IT providers and medical device manufactures as the overall security posture of health care providers is dependent upon the products and applications provided by their vendors.*

Recommendation 2.13: Level of Assurance (LOA) by setting

INSERT TEXT

Action Item 2.13.1: *TEXT*

Commented [JC66]: Comment from Lauren Thompson: Not sure we should tell them how to do it.

Commented [JC67]: Comment from Theresa: We are really going to recommend more audits? I think we will be run out of town for this recommendation. This automatically creates an adversarial relationship

Recommendation 2.14: Drug Enforcement Administration multi-factor example; positive msg; LOA3

Establish guidance to help health care organizations identify the most approach level of assurance for identity proofing.

Action Item 2.14.1: *TEXT*

Recommendation 2.15: Study of $ DIB by sector – can't trust market

Recommend reviewing the investment of small, moderate, and large health care organizations and investments in cybersecurity to evaluate reasonable recommendations and best practices.

Action Item 2.15.1: *TEXT*

Recommendation 2.16: Add interoperability and cyber health survey to MACRA/Meaningful Use reporting survey

Enhance existing MACRA/Meaningful Use guidance to clearly ensure interoperability and cybersecurity are clearly addressed.

Action Item 2.16.1: *TEXT*

Imperative 3. Increase the prevalence of and access to cybersecurity awareness and educational programs across health care industry stakeholders.

INSERT TEXT DESCRIBING THE IMPERATIVE

Recommendation 3.1: Establish a baseline of cybersecurity hygiene within the health care marketplace.

The introduction of health information technology has improved the quality and safety of patient care. There have been unintended consequences, however, that have impacted patient safety. One result has been the effect of health information exchanges on patient privacy and safety. The health care market is currently plagued by a high degree of variability in the understanding of cybersecurity concepts across its breadth of different stakeholders. Patients have some understanding that their individual safety of themselves and their information may be compromised by threat actors. Some health care providers are acutely aware of the issues, while others are either less informed or have inadequate resources to keep pace with the threats. Network infrastructure providers (e.g., networking equipment manufacturers, software vendors, and service providers) sometimes provide robust solutions with strong capabilities to mitigate cybersecurity threats. In some cases, these providers do not appreciate some of the nuances in the practice of medicine or clinical workflows that can affect security (e.g., when there is low visibility into the final system or application). Finally, some medical device manufacturers are proactive and strive to do their part to implement a helpful cybersecurity solution, while others take a "wait and see" position to gauge what the market will demand of them.

It is this high level of variability that necessitates that a baseline of cybersecurity hygiene be established in the health care marketplace. The deployment or implementation of such a baseline can likely best be controlled through its application to new equipment/software entering the market, since patching or replacement are the prevailing options for legacy technologies that are currently operational in the marketplace.

Action Item 3.1.1: *All health care infrastructure technology security should be managed with a focus on patient safety, both on an individual and population basis.*

Action Item 3.1.2: *There should be no known malware in newly produced equipment/software entering the market (i.e., pre-market), and there should be ongoing surveillance for malware in equipment/software currently on the market (i.e., post-market).*

Action Item 3.1.3: *Generate a "Bill of Materials" for newly produced equipment/software entering the market so that components are recognized and assessed against the same cybersecurity baseline requirements as the products into which they are integrated. [Medium Term]*

Action Item 3.1.4: *There should be no common vulnerabilities and exposures with the potential to impact patient safety in critical health care infrastructure technologies (pre- and post-market).*

Action Item 3.1.5: *Common weaknesses should be recognized, characterized, and managed relative to common attack patterns, either during design and development of the technology or*

Commented [JC68]: Comment from Lauren Thompson: This imperative statement doesn't seem to me to speak to the recommendations/action that follow

Commented [JC69]: Comment from David Ting: What do we mean by cyber hygiene? How do this differ from a baseline cyber security requirement as outlined in the NIST CSF? Are we overloading the term?

Commented [JC70]: Comment from Vito: Not clear what the action item could/should be.

Commented [JC71]: Comment from Theresa: FDA needs to take a stronger stance on guidance and become more regulatory for this to occur. Today the market guidance does not include any type of enforcement.

post hoc in the form of compensating controls within the broader system environment into which the technology would be integrated.

Action Item 3.1.6: *For existing and legacy equipment, a systematic approach of patching, compensating controls, isolation, and/or replacement (as available or applicable) should be applied. For newly produced equipment/software entering the market patching capabilities should be in place.*

Action Item 3.1.7: *Full lifecycle security management of critical infrastructure technologies should be instituted, ranging from "concept of operations" to "design and development" to "operation and maintenance" to "decommissioning and disposal."*

Recommendation 3.2: Establish accrediting bodies to improve overall cybersecurity hygiene.

Commented [JC72]: Rather than establishing new accrediting bodies, was there consideration to having existing programs (i.e.: JCAHO - The Joint Commission add this into existing inspections?

While all of these elements and action items of the baseline for cybersecurity hygiene in recommendation 3.1 are certainly desirable, their implementation should take into account the following factors: 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, and 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) which provides a framework for specifying security functional and assurance requirements that independent testing laboratories can evaluate products against.

Under such models, accredited (i.e., normalized) conformity assessment against the baseline for cybersecurity hygiene and accredited third party certification may be used to reduce the overall regulatory burden to regulators themselves in terms of capacity, to technology vendors in terms of time to market, and to health care providers who seek to adopt the technologies. The marking elements of an accreditation model (analogous to having voltage, current, and frequency markings on the back of most certified electrical products) can demonstrate that the cybersecurity hygiene baseline has been met, reducing the need for regulators, vendors, and providers to provide their own assessments of conformance. Different stakeholders need to validate, test, and certify against the baseline throughout the lifecycle (including system development, procurement, deployment, and maintenance). To keep the cybersecurity posture of products reasonably current throughout the lifecycle (following established industry norms including those for safety-critical software quality), the maintenance (market surveillance / adverse event monitoring / remediation) mechanisms of certification can be used.

This can be accomplished by creating a scheme that relies upon 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 against the baseline. These organizations should be able to operate in a federated manner and combine results to facilitate organizations' risk assessments. Such a model has the potential to expedite market adoption of safe and secure innovative new health care technologies that can improve upon the current state of security in this part of our Nation's critical infrastructure.

Commented [JC73]: From Mark J: Do we want to refer to the need for trained end user/site IT people who can appreciate this body of knowledge and use it. Can link with that section so that one recommendation complements the other?

Action Item 3.2.1: *Adopt an existing accreditation process or identify an agency within which to establish a new accreditation framework to support the cybersecurity hygiene baseline.*

Action Item 3.2.2: *This accreditation framework should be responsible for defining and certifying federated operations and exchange of results, including defining any additional technical solutions, such as, standards for exchange formats.*

Action Item 3.2.3: *Develop a business model/incentives to ensure that the testing/validation/certification data is widely available to health care providers, regardless of size and resources.*

Recommendation 3.3: Recommend workshops / support b/w "us" and major hospital insurers

Develop a series of workshops between insurers and major hospitals to help identify key actuarial data, measures, and roadblocks to improving cybersecurity insurance marketplace.

Action Item 3.3.1: *HHS should partner with DHS to further cybersecurity insurance in the marketplace.*

Recommendation 3.4: Consumer grading system; security good

Implement a "consumer reports" or "housekeeping seal of approval" like capability to independently assess and rate consumer health care/lifestyle products. Improve the education of consumers when selecting and using products with security built-in.

Action Item 3.4.1: *Implement a Federal grant to prototype such a group for health care-related technologies. Partner with DHS and the Federal Trade Commission (FTC) for potential broader industry adoption.*

Recommendation 3.5: Education and Awareness campaign – data stratification

INSERT TEXT

Action Item 3.5.1: *TEXT*

Recommendation 3.6: Government and business leaders in health care, information technology, communications, and security and privacy need to work with patients (and all consumers before they become patients) to provide them with better information and training. As a result, patients can make better, more informed decisions about how to handle their health care data and to use "connected health care" responsibility in terms of services, products and providers.

Today, consumers are experiencing near-universal dependence on information technology and information exchange for all aspects of daily life. In no other area is this as critical as in health care. Most consumers are unsure about how to protect their data and personal information. This uncertainty is only exacerbated when consumers become patients and realize concerns about their health, treatments, and costs. Raising cybersecurity awareness will not be confined to health care but it does provide for some ranging from State and Federal regulations to social media and from "wearable" devices ranging from fitness trackers to medical devices and to medico-legal issues around providers having timely, accurate patient information.

Health care will be a special category of increasing awareness but awareness must be coupled with improved security in the hardware, software, and systems utilizing or transmitting electronic protected health information (PHI). Until devices and systems can be made secure, companies at every point on the continuum-of-care must provide training and awareness about products, how their information is shared, and how they can protect or limit its distribution in order to make informed, smart security and privacy related decisions about technology they use and who may access their information.

A recently released report by Rock Health entitled "*2016 Year End Funding Report: A reality check for digital health*" reported, among other key findings, that:

- Digital health reached a tipping point in 2016 as consumers adopted digital health tools at a record rate over the last 12 months. Forty-six percent of consumers are now considered active digital health adopters, having used three or more categories of digital health tools (e.g., telemedicine, wearables)—up from 19 percent in 2015. Only 12 percent of Americans are non-adopters, down from 20 percent in 2015.
- Health data ownership and control is important to consumers, and sharing of health care information is seen as acceptable only in specific use cases. Nearly 87 percent state that they should be in control of who has access to their health data, and almost 86 percent say they should be told what health data is collected about them.

Action Item 3.6.1: *The Task Force supports the Commission on Enhancing National Cybersecurity report's Imperative 3: Prepare Consumers to Thrive in a Digital Age, specifically Action Item 3.1.3 which states: The FTC should convene consumer organizations and industry stakeholders in an initiative to develop a standard template for documents that inform consumers of their cybersecurity roles and responsibilities as citizens in the digital economy – along with a "Consumer's Bill of Rights and Responsibilities for the Digital Age."*

Commented [JC74]: "…provide for some" what? I think there's a word missing here.

Commented [JC75]: Comment from David Ting: Most provider and hospitals ignore patient supplied data since they are liable if they have access to the data but haven't reviewed every second of the supplied data. Unless it is a provider supplied device, not sure if this is a problem yet.

Commented [JC76]: Comment from David Ting: Same comment as above – while patients might have data, providers and hospitals don't want anything to do with it. All the liability with none of the benefits.

Action Item 3.6.2: *HHS should convene patient organizations and industry stakeholders in a similar initiative to develop standard templates for documents that inform patients and caregivers of their cybersecurity roles and responsibilities as patients in a digital health care environment.*

Commented [JC77]: Can this be included with sample HIPAA paperwork? Maybe into 1 document? The push to electronic and a requirement to add paper being handed out may result in pushback.

These templates and documents should not only address issues of privacy and security while in a hospital or under the care of licensed, certified caregiver, but also the entire continuum of care (e.g., wearable devices that transmit health information; health apps on smartphones or other mobile devices; home health; remote monitoring; payers; pharmacies; patient data used in research and other areas where patient information may be collected, shared, stored, or used for analytics of any kind, including population health).

Action Item 3.6.3: *Providers at all levels should incorporate privacy and security training into all patient education modules or courses, as applicable.*

Specific privacy and security training and/or material should be required for applications, devices, portals, and messaging services used by the provider prior to the patient's use of these devices or systems.

Recommendation 3.7: Executive and Board Education

Develop an education campaign to help Executives and Boards of Directors place a value on cybersecurity. By understanding the threat/risk to the organizations mission and profitability more effectively resource cyber. As advocates for organizational resource, IT leadership is not well prepared or equipped for communicating the risks and needs in many cases.

Commented [JC78]: Comment from Jacki: I think we should include table top exercises with IR to be required by this group.

Action Item 3.7.1: *Ensure cyber workforce training and education focuses on executive communication as a important goal.*

Action Item 3.7.2: *Establish reusable messages and talking points that IT and cyber experts can tailor to their organization for leadership communications.*

Imperative 4. Improve sharing and usage of cybersecurity information throughout the entire health care industry.

The CISA legislation passed in December 2015 helped increase the information sharing partnership between the Federal Government and industry. This initial approach was good at sharing data with organizations already resourced and sufficiently large enough to take advantage of this new information. However, a large portion of the health care industry is either a small or moderate-sized business or communication closely with such organization. With one or fewer dedicated cybersecurity experts on staff, these small/moderate organizations can rarely leverage and take advantage of this additional information as they continue to address basic cyber hygiene concerns.

In response to CISA, HHS has been building its capabilities and relationships to support the health care industry by pursuing establishment of a health care cybersecurity integration center, which will bolster health care industry security analytics and strengthen operational relationships to support proactive cybersecurity fusion analysis and automated threat information sharing. The center will focus on improving national health care cybersecurity incident detection, response, and recovery efforts, as well as enhancing and increasing health care industry threat products, services and support. The center will support health care industry voluntary information sharing efforts by connecting to private sector partners to produce automated threat and vulnerability indicators, as part of the DHS Automated Indicator Sharing program. The center will also evaluate ways to partner with health care industry stakeholders to support tailored information to serve the small provider community.

Recommendation 4.1: Enforcement – mandatory disclosure of cyber incidents; quality of care alignment

Require all health care industry (and supply chain) vendors to disclosure cyber security incidents. Because many large-expense health care products (e.g., x-ray) may stay in production for a decade or more, the ability of organizations to balance the mission delivery and operational risks cannot be effectively evaluated. At this time, many organizations lack the knowledge of known cyber incidents with vendors to make informed business decision. Although the liability and regulatory challenges may exist, executives need the data to make risk tradeoffs with the large use of legacy devices and new technology.

Action Item 4.1.1: *Establish mandatory repository for cyber incidents.*

Recommendation 4.2: Voluntary – information sharing; ability to consume; ecosystem challenges – STIX & SIEM (small)

MSSP and health care products need to establish voluntary, automated information sharing capabilities rather than depending on a team of people to process potential threat indicators (e.g. HITRUST MSSP model for small and medium businesses).

Action Item 4.2.1: *Incentivize the adoption of MSSP for small/moderate organizations that support the voluntary information sharing.*

Commented [JC79]: Something is missing here

Commented [JC80]: David Ting comment: Hygiene again – is there a better description?

Commented [JC81]: Comment from Dan M: Probably should point out Action 1.2.3 from the Commission on Enhancing Nation Cybersecurity. Add any other ideas that need to be thrown in to their write up that are healthcare specific

Commented [JC82]: Dan M Comment: I don't see it as a recommendation. STIX already has good support and probably doesn't need more of a push in this doc.

Commented [JC83]: Comment from Theresa: Seems like we are repeating the same recommendations. Could this be changed to incentivize participation information sharing.

Recommendation 4.3: Voluntary – collect data to influence decisions

Work with the insurance industry to help identify and collect actuarial data (?)

Action Item 4.3.1: *TEXT*

Commented [JC84]: Dan M. Comment: 4.1 and 4.3 seem a bit redundant to me. I think 4.1 could include the idea of 4.3 with the overall gist being that everyone needs to get involved in sharing and utilizing

Recommendation 4.4: The health care industry needs to broaden the scope and depth of information sharing and create more effective mechanisms for disseminating and utilizing that data in all subsector components.

The concept of ISACs was first introduced during the Clinton Administration in 1998 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 have strongly endorsed this concept and codified the support through presidential directives and executive orders. In 2015, Congress passed CISA to remove concerns about liability or privacy issues that might hinder the adoption of this concept by industry. The HPH Sector established the NH-ISAC in response to these developments. While the ISAC has made significant progress in a short period of time to facilitate cybersecurity information sharing, there is still a lot more opportunity to improve this concept.

Commented [JC85]: Examples needed?

Action Item 4.4.1: *The NH-ISAC should consider expanding its focus from purely cybersecurity threat, vulnerability, incident data sharing to include information sharing about any hazard that have the potential to disrupt critical health infrastructure.*

This would include sharing information about national disasters, acts of terrorism, pandemic outbreaks, and information regarding incidents in other sectors upon which the health care relies (e.g., energy, communications).

Action Item 4.4.2: *The NH-ISAC should work more closely with smaller providers and delivery organizations to determine the best way to share actionable alerts with these entities since many small businesses lack the automated tools and skilled personnel to translate the often highly technical information that makes up the majority of reporting today.*

Action Item 4.4.3: *HHS, in coordination with DHS, should work to establish prioritized intelligence requirements from each component of the health care industry to serve as triggers for the dissemination of Government threat intelligence to the private sector.*

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 of used by nation state actors to steal intellectual property. These prioritized intelligence requirements can be used to ensure the most meaningful information gets to the right audience in the right time and filter unnecessary information from those that do not need it.

Action Item 4.4.4: *HHS and the NH-ISAC should work with DHS and other entities to develop tools and capabilities that facilitate faster, broader, and more timely dissemination of data across the sector.*

Today, information is often curated and aggregated before being disseminated by both the Government and the private sector entities participating in information sharing mechanisms. This curation can take days or weeks before information is finally shared. We need to be able to respond in near real time to critical threats that are affecting the sector.

Recommendation 4.5: The Federal Government should implement specific requirements that require annual, documented, and tested preparation and readiness exercises for all of the health care industry to ensure all entities are prepared to respond to a significant cyber incident.

The health care industry is a component of critical infrastructure; and as such, resilience to attack is paramount. Even a small loss in capability or loss in health care data can have significant impact in patient care and trust. Current planning and practice for a cyber incident is insufficient within health care, and a significant event would produce an uncoordinated and ineffective response.

According to a various published studies, more than 70 percent of firms surveyed stated that they have Incident Response (IR) Plans in place; yet, less than 15 percent of these organizations review or exercise their plans annually. Incident Response Plans sitting on a shelf and gathering dust without regular review and testing put the health care industry at risk. Cyber response within health care should be made as practiced and planned for as other incidents that can impact health care, such as fast-spreading viruses or prescription drug contamination.

Generic critical infrastructure response plans already exist and should be tailored to the health care industry, and they should be exercised regularly and applied to varied scenarios. The response plans and exercises need to be representative of the complexity involved within health care accounting for the interaction of many subsectors; large supply chain; regional, national and global attacks; as well as the difficulties in response that the convergence of information technologies and physical systems have. Also, clear operating authority should be outlined and clear guidance should be given on where the private sector should go for information and assistance.

Action Item 4.5.1: *The Secretary should implement requirements that each health care entity, regardless of size, have a documented, detailed, and robust Cybersecurity Incident Response Program.*

Action Item 4.5.2: *Such programs should be subject to continued review, update, and revisions based on the changing threat landscape and evolution of the organization.*

Action Item 4.5.3: *At a minimum, the Incident Response Program should be tested at a two tier level once per year.*

Tier One: Each organization will conduct, and fully document, an internal table top exercise of the appropriate size, scale, and scope to ensure principals of the health care organization

Commented [JC86]: This used to be recommendation 3.5

Aftin suggested revising this entire imperative – form this recommendation through the end is what she recommended.

Commented [JC87]: Comment from Theresa: Not sure I like a government mandate here unless other items have occurred. I think we have to be careful about mandating things like this if incentives and rest of recommendations are not implemented. Just creates a scenario for failure. We should caveat this recommendation. I would hate for this one to get pulled out and be the only thing implemented.

Commented [JC88]: Comment from David Ting: Hospitals are required to have Emergency preparedness documents to deal with all types of contingencies – are cyber incidents covered by them and if they are not would this be the ideal place to hang these?

Commented [JC89]: Comment from Mark Jarrett: What about small practices, etc. Works for organizations. Again concept of "local pods" of small providers working together (with Stark exception again)

Comment from Theresa: I agree…I think we have to be careful about mandating things like this if incentives and rest of recommendations are not implemented. Just creates a scenario for failure. We should caveat this recommendation. I would hate for this one to get pulled out and be the only thing implemented.

understand what is required of them and their teams in response to a breach, potential breach, or cybersecurity threat incident.

Tier Two: Each organization will participate in at least one local, regional, or national simulated cybersecurity breach exercise in order to demonstrate their ability to coordinate and communicate externally and across the health care ecosystem. This requirement may be fulfilled by participation in an exercise with HHS or other Federal entities, with existing ISAO or ISAC facilitators, or in a manner organized independently among other participants. In all instances, the details of the annual exercise will be documented and retained for review by HHS officials in the event necessary.

Recommendation 4.6: Strengthen coordination within government and between the public and private sector on activity related to incident response for the HPH Sector.

Commented [JC90]: This used to be recommendation 3.6

Aftin suggested moving

The HPH Sector has been reportedly one of the most targeted critical infrastructure sectors by malicious cyber actors in the past few years. The DHS NCCIC, designated as the Government's 24/7 cyber situational awareness, incident response, and management center providing assistance to potentially impacted entities in their recovery from an incident, works in close coordination with other agencies and the private sector.

Consistent and formal links between the NCCIC and HHS as the Sector Specific Agency during steady state, will help ensure that sector-specific expertise and valuable relationships are effectively being leveraged when incident-related technical assistance is deployed in the HPH Sector. Further, sector-specific expertise unified at the time of Government response team deployment and promulgation of technical assistance lessons learned, can result in more effective efforts to mitigate and prevent the impacts to a cyber attack.

Action Item 4.6.1: *Confirm that the most effective lines of communication and collaboration are established within Government to leverage HPH expertise in incident response.*

HHS as the Sector Specific Agency and DHS/NCCIC should consistently maintain unified and dedicated channels during steady state as well as response between them to: 1) infuse subject matter expertise into issues that involve the HPH Sector; 2) leverage existing sector relationships across Government, within industry, and with a potentially impacted entity; and, 3) facilitate and guide effective and targeted dissemination of resulting clarification and near real time notifications to the sector in a strategically sequenced manner.

Commented [JC91]: Comment from Thad/OCIO: OCIO: HHS healthcare cybersecurity integration center will provide personnel to maintain a dedicated channel with the NCCIC, which will help increase the subject matter expertise and strengthen the operational relationships between HHS and DHS

Action Item 4.6.2: *Strengthen engagement between the public and private sector in HPH incident response.*

HHS as the Sector Specific Agency and DHS/NCCIC should deepen relations with ISAOs focused on the HPH Sector, to leverage NCCIC technical assistance and role of Government in assisting with recovery across the sector. Greater frequency of Government and HPH sector response interaction will enable strategic, near real time dissemination of insight gained, further develop HPH sector-related expertise among Government technical assistance teams, and strengthen cyber defenses, as well as drive innovation across the sector and its broader dependency network.

Commented [JC92]: Comment from Thad/OCIO: OCIO: HCIC will support proactive cyber threat analytics, deepen related activity with the HPH ISAOs

Recommendation 4.7: Establish a MedCERT to coordinate responses cybersecurity incidents and vulnerability disclosures.

Computer Emergency Response Teams (CERTs) coordinate responses to computer security incidents and work with stakeholders to address software vulnerabilities. Currently there is no single cybersecurity incident coordination point for the HPH Sector and those coordination points do not always have the necessary expertise to understand the unique health care impacts. Standing up a Medical CERT (MedCERT) would improve incident response and coordinated vulnerability disclosure across the HPH Sector. 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. The MedCERT will 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. One of the key roles of the MedCERT would be to assign Common Vulnerabilities and Exposures (CVE) identifiers for health care system vulnerabilities, including those discovered in medical devices, health IT systems (e.g., EHRs, EPCS, PACS), mobile applications, and medical Internet of Things. The MedCERT would also coordinate with private industry and Government to assess and adjudicate these vulnerabilities (including the health care impact), compute a CVSS score, and disseminate timely information. The MedCERT would also coordinate with private industry and across the Government to provide public fixes (patches and mitigation strategies) to these vulnerabilities and additional support for incident response in a timely manner.

Action Item 4.7.1: *A MedCERT should be established, as a single organization or as a coordinated activity across multiple entities.*

Action Item 4.7.2: *Expand CVE/CVSS to include medical devices and medical Internet of Things for vulnerabilities in software, hardware, and firmware.*

Action Item 4.7.3: *Since medical devices and health IT systems contain third party software, the MedCERT needs to correlate the vulnerabilities found in this third party software, which are enumerated in the National Vulnerability Database.*

Action Item 4.7.4: *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 the independent certification and testing capabilities described in Recommendation 6.2. These technical analyses provided by individual testing labs will need to be correlated to support the MedCERT's vulnerability validation and assessment roles.*

Imperative 5. Consider the unique challenges for health delivery organizations and small providers and develop incentives to increase overall cybersecurity posture.

INSERT TEXT DESCRIBING THE IMPERATIVE

Recommendation 5.1: Legacy – IT refresh; incentives

For many of the health care provider services, operational budgets for IT may only reflect four percent of an organization budget. IT security comes out of that overall IT budget and appears lower than other industries. In addition, large investment costs in health care IT (e.g., x-ray machines, ambulances) create a large legacy devices/IT component that cannot be or cannot easily be secured. Organizations need to be incentivized to migrate from less secure legacy systems.

Action Item 5.1.1: *Implement a "cash for clunkers" model for large expensive medical devices. Use funding to remove unsecure devices from the U.S. marketplace and provide partial funding for more effective and more secure current technologies. [Medium Term]*

Action Item 5.1.2: *Implement a revolving fund, like the proposed Federal IT modernization fund, to help hospitals replace obsolete IT devices and use future year O&M savings to reimburse the revolving fund.*

Commented [JC93]: Potential to remove this imperative since other recommendations suggested moving to other imperatives

Commented [EC94]: Do we have any data we can quote in this area?

Commented [JC95]: Comment from Aftin: Recommendation deleted because this information was already being discussed in the medical device section and so this text was incorporated into the incentives section of the medical device section

Imperative 6. Increase the security and resilience of medical devices and health technology.

The cybersecurity of networked medical devices and other software or systems that connect to the EHR is paramount because of the potential impact to patients. The HPH Sector is charged with keeping patients safe and that includes protecting patients from physical as well as privacy related harms that may stem from a cybersecurity vulnerability or exploit. If exploited, cyber vulnerabilities may result in medical device malfunction, disruption of health care services (including treatment interventions), inappropriate access to patient information, or compromised EHR data integrity. Such outcomes could have a profound impact on patient care and safety.

One foundational challenge that will need to be addressed in order to enhance the cybersecurity of medical devices and EHRs is unsupported legacy operating systems. The relatively short lifespan for operating systems and other relevant platforms such as commercial off the shelf (COTS) software is inherently misaligned in HPH as medical devices and EHRs may be utilized for 10, 15, or 20 or more years. This misalignment may occur for a variety of reasons including HDO resources (hospitals are operating on thin budgets and cannot replace capital equipment like MRIs as quickly as new operating systems are released), product design lifecycle (product vendors have a product development lifecycle which may take several years and thus they may start development using one operating system and by the time the product comes to market, newer operating systems may be available), etc. Creative ways of addressing this challenge may be found by engaging key industry stakeholders including software vendors.

Though unsupported legacy operating systems are a foundational challenge, other key challenge areas exist that if addressed have the potential to positively impact medical device and EHR cybersecurity. The challenge areas that are being highlighted were selected because they were thought to have the highest potential for large scale impact if they could be addressed. However other challenge areas exist and in order to comprehensively enhance medical device and EHR cybersecurity these will need to be addressed as well. Highlighted challenge areas include: 1) securing legacy systems; 2) implementation of a secure software development lifecycle (SDLC); 3) strategic and architectural approaches to the deployment, management, and maintenance of medical devices; and 4) incentives for enhancing medical device and EHR cybersecurity. There is an additional challenge area that is EHR-centric concerning holistic data flow and system requirements that do not negatively impact the clinical workflow. Though the actions for achieving the forthcoming recommendations are unique, the ultimate objective of enhanced patient safety is the same. Please note that the recommendations provided herein are not singular solutions and are expected to have cascading effects. For example, the implementation of recommendations in the area of secure SDLC today is expected to have positive impacts on future legacy systems as these would have more built-in security features and thus provide better "security longevity". Recommendations regarding the aforementioned challenge areas, the desired end state, and proposed action items for how this desired end state may be achieved are provided below.

However, it should be noted that the recommendations provided herein are not singular solutions and are expected to have cascading effects. For example, the implementation of recommendations in the area of secure SDLC today is expected to have positive impacts on future legacy systems as these would have more built-in security features and thus provide better "security longevity". The challenge areas that have been highlighted were selected because they

Commented [JC96]: Comment from Aftin: CHCA recommended awareness of need for clarification with respect to dealing with a certain class of apps, devices and systems which operate under consumer-authorization rather than provider authorization. This feedback was given in the context of EHRs. What are thoughts on describing consumer devices in the scope of our discussion? If we should include it, thoughts on how we might do so?

were thought to have the highest potential for large scale impact if they could be addressed. However other challenge areas exist and in order to comprehensively enhance medical device and EHR cybersecurity these will need to be addressed as well.

Recommendation 6.1: Legacy systems need to be secured.

Legacy medical systems include both legacy medical devices and legacy EHR applications which may not have any ongoing software support from the hardware and software vendor(s), for the full system: Hardware BIOS & Drivers, Operating System and all Applications in use.[29],[30] These legacy systems have security weaknesses, which may compromise the hospital network. It is desired that every vendor and health care organization should be able to identify and classify legacy systems and develop an approach (compensating controls, device update or retirement, etc.) to mitigate the risks associated with these legacy systems. Please 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 6.1.1: *Stakeholders (manufacturers, vulnerability finders, etc.) should engage in coordinated vulnerability disclosure and manufacturers should adopt coordinated disclosure policies.*

While coordinated disclosure policies are gaining traction in health care and public health, widespread adoption might be accelerated if commonly used standards were made publicly available. Thus as a part of this action item, it is recommended that the appropriate standards bodies make ISO/IEC 29147 (Information technology – Security techniques – Vulnerability disclosure) available at no cost.

Action Item 6.1.2: *Stakeholders (manufacturers, HDOs, researchers, etc.) should actively participate in Information Sharing and Analysis Organizations (ISAOs)*

Information sharing is critical to the adoption of a proactive approach to cybersecurity. Sharing of cybersecurity vulnerabilities and intelligence aids in the management of individual cybersecurity vulnerabilities and provides advance threat information to the HPH Sector as a whole. For additional information and recommendations on information sharing, see Imperative 4 of this report.

Action Item 6.1.3: *Medical device manufacturers should create a bill of materials that describes its device software components as well as any known risks associated with those components. [Medium Term]*

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 HDOs in the management of 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

[29] Note that there are several types of legacy products including legacy systems that are still be reported 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.
[30] Note that devices may be legacy but still have patches available.

on their networks and enables providers to implement mitigation strategies when patches are not available. To date, this practice has not been widely adopted.

Action Item 6.1.4: *For devices that are still receiving some support from the device manufacturer and/or application vendor, it is recommended that these organizations make real time updates and patches (e.g. to the operating system, etc.) as well as compensating controls available to end users. HDOs should also have a policy/plan in place to be able to receive and implement available updates.*

The product vendor should be transparent about their ability to patch and update products during the procurement process. This includes relaying to potential customers the amount of time remaining for product support during procurement. Additionally, HDOs should ensure that their systems and policies account for the implementation of updates and patches which may be available.

Recommendation 6.2: A secure SDLC should be used 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 life cycle (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 vulnerability in the system.[31] 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 not only to manage and eliminate vulnerabilities in the system, but they would also communicate the dispositioning of vulnerabilities and the identification of new vulnerabilities to all appropriate stakeholders, enabling responsibility agreements[32] and policies that that would help to provide the necessary security and privacy assurances. Taken together, secure SDLC activities would help to reduce safety risks, which is of paramount importance in protecting patients.

Action Item 6.2.1: *Manufacturers should implement security by design and throughout the product lifecycle*

The adoption of these secure SDLC practices (such as no longer using hardcoded passwords) will enhance product security by making them less susceptible to distributed denial-of-service (DDoS) attacks such as the Mirai botnet as an example.[33] Several secure SDLC models may be leveraged by industry to enhance the cybersecurity of their products. The basic steps within these models include gathering requirements, designing a software blueprint, generating source code, testing and verification, and deployment. This should be a continuous improvement process with

[31] NIST. (2008). *NIST Special Publication 800-64 Revision 2: Security Considerations in the System Development. Life Cycle*. Retrieved from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf
[32] ISO. (2010). *IEC 80001-1:2010 Standard*. Retrieved from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863
[33] US-CERT. (2016, October). Alert (TA16-288A): *Heightened DDoS Threat Posed by Mirai and Other Botnets*. Retrieved from: https://www.us-cert.gov/ncas/alerts/TA16-288A

information gleaned from deployment impacting future requirements and thus the rest of the secure SDLC process. Security throughout the product lifecycle also includes the incorporation of third party software and components. FDA has provided guidance[34] to medical device manufacturers regarding cybersecurity and risk management concerning the incorporation of OTS software. It is important that manufacturers account for supply chain risks in their lifecycle management

Action Item 6.2.2: *Vendors, HDOs, and other HPH stakeholders should work together to identify cybersecurity baselines for networked devices which can then be extrapolated out on a product-product basis based on specific hazards or threat models associated with product usage.*

Industry is already starting some of this work for medical devices through efforts such as AAMI TIR 57, UL 2900,[35] and DTSec's[36] cyber security standards initiative. However, a gap exists at the interface between medical devices and EHRs because regulatory boundaries are crossed. Thus the baselines that are developed will need to meet the requirements of several regulatory bodies. Additionally interfaces between medical devices and non-regulated systems such as IT networks should be considered. Stakeholder baselines are further bolstered by the use of accreditation models which could evaluate product performance against the identified security requirements within a system of systems which may include both medical devices and EHRs. For additional information and recommendations on cybersecurity accreditation and testing see Imperative 3 of this report.

Action Item 6.2.3: *Vendors, HDOs and other HPH stakeholders undertake a gap analysis of the common vulnerability scoring system (CVSS).*

This action would be valuable as there may be difficulty managing cybersecurity vulnerabilities to clinical hazards. CVSS and other scoring systems serve as indicators of risk which are input into an organizations risk assessment process. Specifically, vendors, HDOs, and HPH stakeholders would work together to determine what medical device-specific information is needed for these scoring systems in order to aid in the assessment of clinical impact when assessing vulnerabilities during the design process and when vulnerabilities are found after deployment. Other gaps within the existing CVSS platform for medical device risk assessment that may warrant additional stakeholder discussion include chained vulnerabilities, assessing environmental impact, and limitation of the CIA triad for medical devices. A CVSS assessment of a single vulnerability may be influenced by other vulnerabilities that exist in the system and thus it would be important for stakeholders to discuss how the chaining of vulnerabilities impacts assessment. Discussion of how to best account for the varied clinical environments in the assessment would also be of high-value.

[34] FDA. (1999). *Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices*. Retrieved from: http://www.fda.gov/downloads/MedicalDevices/.../ucm073779.pdf
[35] UL. (2016). *UL Launches Cybersecurity Assurance Program*. Retrieved from: http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/
[36] Diabetes Technology Society. (2016). *New Standard to Raise Confidence in the Security of Network-Connected Medical Devices through Expert Evaluation*. Retrieved from: https://www.diabetestechnology.org/dtsec.shtml

Recommendation 6.3: Employ strategic and architectural approaches to reduce the attack surface for medical devices, EHRs, and the interfaces between these products.

An overall strategy and architectural approach provides an important foundation that supports the deployment of medical devices and EHRs. This approach includes considering the long-term viability, effectiveness, security, and maintainability of those products when setting up the IT network and at the outset of product deployment. This strategy can be specific to the medical device and EHR deployment, or it can be part of a broader technology strategy that includes a component for the medical device(s). Both the device vendor and HDOs using the product must assume key responsibilities in order to reach the desired end state of having every product (whether new or when it is being upgraded) having a defined strategy and architectural approach and design that supports the deployment and overall lifecycle management of that product.

Action Item 6.3.1: *HDOs should develop a holistic strategy to build, validate, and test the infrastructure needed to support secure installation, connectivity, and configuration of products.*

Such a strategy would allow hospitals to better account for security patches and updates to their systems because they would be thinking about including these capabilities at the outset of their network development. As a part of this strategy development, consideration could be given to having a full test network which would be valuable as more robust testing could be completed without compromising live networks/systems. This approach is also more holistic as it enables assessment of a system rather than just looking at a single component Furthermore, a holistic strategy would allow hospitals to develop more robust system architectures such that even if a device on a network is compromised, the impact of the device on the network and other workflows upstream could be minimized. Technical controls including firewalls, access control lists, etc. may also be leveraged as a part of this holistic strategy. With regard to EHRs specifically, having EHR vendors specify their operating systems would aid hospitals in the implementation of their strategy.

Action Item 6.3.2: *Manufacturers should provide network instructions for use (i.e., instructions for device installation, including device configuration and network connectivity requirements, documentation on secure preparation for recycling or disposal of medical devices) and specific guidance regarding supporting infrastructure architecture (e.g., network segmentation requirements). [Long Term]*

Ideally these instructions would include how to scrub any personally identifiable information or PHI or other site-specific sensitive data such as configuration files.

Action Item 6.3.3: *Medical device manufacturers, EHR manufacturers, and their regulators should have a stakeholder meeting to get a better understanding of the product interdependencies and identify opportunities for stakeholder collaborations.*

It is recognized that EHRs and medical devices may interface directly and as a result the data flows and security of one product type impacts the other. For example, the medical device may have a "back door" for diagnostics or other purposes that may send data back to the medical device company or third party. This integration and two-way data flow increases cybersecurity risks to patient data and patient safety. The security of these technologies is further complicated because there is not a single regulatory framework for medical devices and EHRs as they fall under the regulatory purview of different regulatory agencies. Additionally, the interfaces of

these technologies may not be fully encompassed within either of the existing frameworks which may result in cybersecurity gaps. Finally, these technologies are often assessed in isolation which is not reflective of the interconnected space in which they operate. Increased engagement and collaboration, and discussion among key stakeholders of these and other cybersecurity challenge areas impacting medical devices and EHRs is expected to result in enhanced cybersecurity for these systems of systems.

Action Item 6.3.4: *Cybersecurity surveillance of medical devices and EHRs once they are deployed.*

There is a need to determine whether the functionality of these products is impacted by cybersecurity threats and risks. Supporting the advancement of a proactive, national surveillance such as a National Healthcare Technology Cyber and Safety Network (e.g., something like the National Health and Safety Network[37] used for the Centers for Disease Control and Prevention to track hospital acquired infection risk) would be of value. However in order to undertake surveillance, you need to have the capability to detect a cybersecurity concern and having hospitals and product vendors adopt a program like the DHS Continuous Diagnostics and Mitigation (CDM) program would help. The benefits of surveillance could be further realized if product vendors incorporated detection mechanisms and features into their device design.

Action Item 6.3.5: *Advance data standard use-cases to mature the integration of data standards.*

The value of any surveillance system is only as good as the quality of the data that enters that system. Enhancing the data quality of cybersecurity threat and vulnerability information coming into various nodes in the HPH ecosystem is expected to increase the quality of cybersecurity threat intelligence, device adverse event reporting, etc.

Recommendation 6.4: Integrate the management of medical devices with IT.

Commented [JC97]: This used to be recommendation 5.3 – Aftin – recommended moving

Currently, medical devices are managed by a separate department such as Clinical Engineering. We have been seeing an exponential increase in medical devices with network capability. A knowledge of IT and support from IT teams is required to implement an effective and robust security program for medical devices with network capability.

Action Item 6.4.1: *Health care providers should ensure that their Clinical Engineering/Medical Device management resources have sufficient level of IT support and strong exposure to IT and cybersecurity related controls.*

Action Item 6.4.2: *Health care providers should consider integrating their biomedical engineering with their IT resources to provide robust support in maintaining medical devices with network capability.*

Action Item 6.4.3: *The Bio-Medical Engineering team within health care providers should collaborate with their IT resources during the selection of new medical devices and technologies to ensure that appropriate IT and cybersecurity controls are addressed upfront.*

[37] Centers for Disease Control and Prevention. (2015, October). *About National Healthcare Safety Network*. Retrieved from: https://www.cdc.gov/nhsn/about-nhsn/index.html

Action Item 6.4.4: *The Bio-Medical Engineering team within health care providers should collaborate with their information security groups in addressing risk assessments and ongoing cybersecurity monitoring for medical devices.*

Recommendation 6.5: Industry incentives should be developed to enhance the medical device and EHR ecosystem.

For many of the health care provider services, operational budgets for IT (including cybersecurity) may only reflect 4 percent of an organization budget. In addition, large investment costs in capital equipment create a large pool of legacy devices/IT that cannot be or cannot easily be secured and the product updates/patches needed to secure these systems result in increased costs for product vendors. Organizations need to be incentivized to migrate from less secure legacy systems. The use of incentives could be particularly useful if leveraged as a strategic approach to achieve a desired end state where legacy systems are removed from the market and replaced with systems with improved cybersecurity. A risk-based approach could be leveraged and within this framework, legacy health care technology would be replaced with technology that adheres to certain risk management and technical standards in health care provider environment such as IEC 80001,[38] AAMI TIR57,[39] NIST SP 800-53,[40] ISO 27001,[41] etc. It should be noted that the impact of this recommendation is dependent upon the timing in which it is employed, with the greatest value add of this approach being realized if it is employed several years after the widespread adoption of secure SDLC and strategic/architectural approaches. Doing so will help to ensure that the replacement devices inherently have better cybersecurity and may be deployed in the health care environment via the use of enhanced cybersecurity practices. Incentivizing the use of compensating controls that reduce cybersecurity risks without completely removing the technology may also be of value. In addition to the buy-back programs, reimbursement, insurance, and tax incentives could also play a role. However, it is noted that new incentive approaches would have to be evaluated to ensure that they did not cause conflicts for existing compliance rules such as the Anti-Kickback Statute.[42]

Action Item 6.5.1: *Government and industry need to come together to brainstorm incentive models for consideration. [Short Term]*

Potential incentive models that may be considered include but are not limited to a one-time buy-back program such as cash for clunkers,[43] phased approach for replacing legacy systems with ones that adhere to certain risk management and technical standards in health care provider

[38] ISO. IEC 80001-1:2010: *Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities*. Retrieved from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863
[39] AMMI. *AAMI TIR57: Principles for medical device security—Risk management*. Retrieved from: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729
[40] NIST. *NIST Special Publication 800-53 (Rev. 4)*. Retrieved from: https://web.nvd.nist.gov/view/800-53/Rev4/home
[41] ISO. *ISO/IEC 27001 - Information security management*. Retrieved from: http://www.iso.org/iso/iso27001
[42] American Health Lawyers Association. (1999). *Anti-Kickback Statute*. Retrieved from: https://www.healthlawyers.org/hlresources/Health%20Law%20Wiki/Anti-Kickback%20Statute.aspx
[43] Department of Transportation – National Highway Traffic Safety Administration. (2016, May). *Car Allowance Rebate System (CARS) – Transactions*. Retrieved from: https://catalog.data.gov/dataset/car-allowance-rebate-system-cars-transactions-final-paid-transaction-database-mdb-file-via-e0bae

environments that adhere to standards such as the Montreal Protocol,[44] or an ongoing buyback/upgrade program such as a revolving fund[45] like that proposed by the Federal IT modernization fund. One aspect of the Montreal protocol includes establishing centralized funding for health care providers to make a capital investment. A revolving fund like the proposed Federal IT modernization fund could help hospitals replace obsolete IT devices and use future year O&M savings to reimburse the revolving fund. As a part of brainstorming activities, government and industry should ideate on how incentive structures for replacing devices as well as instituting compensating controls that result in more effective and more secure technologies might be funded (e.g. government and industry collaborations, tax incentives, etc.). Another topic to be considered during these discussions is potential implementation barriers.

Action Item 6.5.2: *Government should considering issuing a grand challenge, soliciting from stakeholders novel incentive structures that could be leveraged to address cybersecurity challenges specific to securing legacy systems, secure SDLC, strategic and architectural approaches, and holistic data flow and system requirements for EHRs.*

Recommendation 6.6: Holistic data flow and system requirements should allow for data security without negatively impacting the clinical workflow (note that this recommendation is EHR-centric)

EHRs are now used ubiquitously in health care with the intent of enhancing patient care. While the digitization of patient records aids interoperability, it also increases the attack surface for health care systems and patients. Numerous individuals and entities internal and external to an HDO such as physicians, nurses, CMS, and the Joint Commission need access to EHR data. It is desired that the data is secured such that the clinical workflow is not negatively impacted and that each participant in the data flow chain has appropriate security safeguards and requirements.

Action Item 6.6.1: *HDOs, EHR vendors, and the Government work together to improve management of EHR access internal to a facility and on the management of data flows outside of a facility.*

The level of security that can be utilized for data flow is limited by the security capabilities of the least cyber-mature organization in the data exchange. Raising the baseline level of security of the parties exchanging EHR information such that they are capable of using encryption and other data security techniques would be of benefit. The integration of medical devices and EHRs also represents a risk to data flow and management as the interfaces between these products often requires a third-party interface which may be less secure. Thus the possibility of two-way communication between the medical device and the EHR leads to a need to directly, and more securely integrate medical devices with EHRs. This interface and integration is a critical aspect of discussion going forward.

[44] Multilateral Fund. *Montreal Protocol*. Retrieved from: http://www.multilateralfund.org/default.aspx
[45] Information Technology Modernization Act. (2016). Retrieved from: https://www.congress.gov/bill/114th-congress/house-bill/4897/text

Action Item 6.6.2: *HDOs should improve their internal EHR access management through the use of security requirements including two-factor authentication, assignment of privilege, and ultimately a more robust Identity Access Management (IAM) set of solutions.*

The impact of EHR security requirements on the interaction/interface of this technology with medical devices should also be considered.

Recommendation 6.7: Establish a medical device-specific MedCERT to coordinate responses cybersecurity incidents and vulnerability disclosures.

In Imperative 4 of this report, it was recommended that a MedCERT be stood up for the entire HPH ecosystem as a single coordination point. While this recommendation is valuable for the sector as a whole, there is a need for MedCERT that is specifically focused on medical devices because of the inherent impacts to patient safety when vulnerabilities are disclosed and/or exploited. The medical device specific MedCERT would be comprised of medical device engineering, software, hardware, clinical (e.g. physicians and nurses), biomedical engineering (e.g. hospital biomeds), and security expertise. Having breadth and depth of expertise would enable this group to comprehensively coordinate responses. As a part of its vulnerability disclosure function, this team would help to assess the vulnerability, evaluate patient safety risk, serve as an adjudicator between the vulnerability finder and the product manufacturer, assess proposed mitigations, 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 which could be deployed in the field to investigate., This group would be tasked with coordinating a response.

Action Item 6.7.1: *Industry and government should have a stakeholder meeting to discuss the features, capabilities, and operationalization of a medical-device specific MedCERT.*

Recommendation 6.8: Conduct threat modeling and identify potential threats to medical devices during the design phase.

Identifying potential threats to a device at design time is critical to protecting against those threats. Patients need to have confidence that the devices used in the delivery of their health care services are safe, and that those devices do not themselves pose a threat to their health. These interconnected medical devices present numerous security risks including susceptibility to malware infections, vulnerability to hacking, and often provide an entry point into a hospital's network for unauthorized access. These vulnerabilities pose multiple threats to the security, confidentiality, integrity, and availability of health information.

Premarket[46] and Postmarket[47] management recommendations issued by the FDA advocate that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of the SDLC. While threat modeling is most impactful during the earliest stages of a health care IT project, it should be addressed continuously throughout the SDLC.

The FDA should require the use of threat modeling to optimize network/application/Internet security by identifying objectives and risks, and then defining counter measures to prevent, or mitigate the effects of, threats to the systems.[48]

Action Item 6.8.1: *With the increase in connected devices comes a corresponding increase in potentially vulnerable devices on a hospital network. In order to understand the risks presented by a medical device, identification of the cyber threats and weaknesses must be performed. Many medical device manufacturers perform no threat modeling on their products as part of the SDLC.*

Federal Agencies (i.e., FDA and HHS) should require the use of threat modeling by medical device and EHR companies and manufacturers to strengthen security by identifying cyber threats and weaknesses to their products and product line.

[46] FDA. (2014, October). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
[47] FDA. (2016, December). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Retrieved from: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
[48] Open Web Application Security Project. (2016, August). *Threat Modeling*. Retrieved from: https://www.owasp.com/index.php?Category:Threat_Modeling

Imperative 7. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.

The health care industry is the largest investor in R&D in the U.S. The value of intellectual property is undermined through constant cybersecurity attacks.

Recommendation 7.1: Long-term implications and loss

Develop guidance on evaluating potential economic impact and loss for cybersecurity risk for health care research and development. Providing the resources to more adequately evaluate the risk when organization leadership is resourcing IT and cybersecurity.

Action Item 7.1.1: *Establish a task force to develop risk models for evaluating U.S. economic and organizational impact for cybersecurity failures.*

Recommendation 7.2: Teaching institutions; medical school attached/affiliated; medical facility; Penn Hershey example

The attack surface of joint education institutions and medical services is often at heightened cybersecurity risk. As staff work in the education, research, or health care services aspects of the organization the architecture and design of security controls may not always be prioritized based on potential economic impact.

Action Item 7.2.1: *Support the development of best practices to balance the encouraging of academic freedom, ensure protections of intellectual properties from research, and to deliver quality health care services.*

Recommendation 7.3: Health care S&T; grand challenge incentives

Fund the research and development of innovative solutions for supporting small, moderate and rural organizations. The DHS Science and Technology (S&T) organization already coordinates small investments in areas such as medical devices but significantly more investment should be made. Help pilot and transition these solutions to address the pressing need of the health care industry.

Action Item 7.3.1: *HHS funding for cybersecurity research increase and innovative solutions such a grand challenge.*

Action Item 7.3.2: *HHS partner with DHS S&T to prioritize and implement new research to support small and rural organizations.*

Recommendation 7.4: 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. 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 provided a security clearance. However, it is important to establish mechanisms for prioritizing clearances for those with the greatest ability to act on cyber threat information to reduce cyber risks to the nation's health care system.

Action Item 7.4.1: *HHS, DHS, and 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.*

Such clearance should not be dependent on the qualifications of other senior executives or corporate board members of the respective health care organizations. Participants in the program should retain the secrecy of the intelligence until such time as the information becomes public. Participants can utilize the information to execute countermeasures within their respective organizations.

Recommendation 7.5: Security for BIG data sets versus speed/priorities

Fund solutions, like shared service providers, to build secure models/frameworks for sharing big data necessary for medical and health care research. The academic and health care industries currently may be risk adverse to implementing large data sharing initiatives without proven cybersecurity protections.

Action Item 7.5.1: *TEXT*

VII Next Steps

INSERT TEXT

Commented [JC98]: Thad/OCIO Comment: HHS OCIO: Suggest that, as part of the next steps the TF consider language that Congress should evaluate what resources are needed to support the recommendations, to ensure the department can deliver, prioritize or align resources where needed, or be funded to create new capabilities such as the healthcare cybersecurity integration center

Appendix A. Acronyms

ASPR	Assistant Secretary for Preparedness and Response
CIO	Chief Information Officer
CISA	*Cybersecurity Information Sharing Act of 2015*
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
DHS	U.S. Department of Homeland Security
EPCS	Electronic Prescribing of Controlled Substances
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
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
HPH	Health Care and Public Health
IR	Incident Response
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organizations
MACRA	Medicare Access and CHIP Reauthorization Act
MSSP	Managed Security Service Provider
NCCIC	National Cybersecurity and Communications Integration Center
NH-ISAC	National Health - Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
ONC	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
R&D	Research and Development
SDLC	Software Development Lifecycle
U.S.	United States

Appendix B. Task Force Background and Approach

To accomplish its goals and charge under CISA Section 405, HHS established the HCIC Task Force and selected members representing a wide variety of organizations to include Federal personnel, hospitals, insurers, patient advocates, security researchers, pharmaceuticals, medical device manufacturers, health IT developers and vendors, and laboratories. These individuals possess a breath of deep expertise in information and cybersecurity, clinical medicine, medical device development, and software development. HHS selected Task Force members based on recommendations from a panel of subject matter experts from HHS, DHS, and NIST based on the following criteria:

- Service in a position of influence in an organization that is representative of a component of the broad health care and public health sector;
- Experience in dealing with technical, administrative, management, and/or legal aspects of health information security;
- Knowledge of major health information security policies, best practices, organizations, and trends; and
- Ability to participate actively in Task Force meetings and contribute to products.

The Task Force formalized its approach to meeting the CISA requirements by holding monthly meetings over the course of one year. In an effort to engage the public in the discussion and gather insights from outside of the immediate membership, the Task Force held four in-person meetings where a portion of each meeting was open to the public and media. To focus and streamline its efforts, the Task Force also established independent workstreams to address different issues related the health care and cybersecurity in relation to its charge under CISA.

Subject matter experts within and outside the Task Force, coordination with other critical infrastructure sectors, Task Force workstreams, and independent research informed the development of this report and recommendations. Due to the timeframe in which the Task Force had to conduct its examination, it elected not to evaluate or make recommendations about the medical device aftermarket or [OTHER AREAS THE TASK FORCE ELECTED NOT TO ADDRESS].

Commented [JC99]: Insert other areas. International issues?

Risk Workstream: The Risk Workstream coordinated with representatives from across the various subsectors of the health care industry to examine and identify risks to confidentiality, availability, integrity, and patient safety. Topic areas for identified risks ranged from research and development, sales and distribution, diagnostics and results distribution, claims processing, to corporate functions depending on the specific subsector.

Communications Workstream: The Communications Workstream leveraged Reddit, LinkedIn, and blog posts to coordinate with and gain feedback from the public on issues for Task Force consideration; identification of risks, threats, and vulnerabilities to the sector; and recommendations for areas where the public would like to see Congressional action. The results of these efforts informed Task Force discussions and the development of recommendations.

Medical Device Workstream: The Medical Device Workstream identified problem statements and a desired end-state for the secure SDLC, legacy devices, strategic and architectural approaches for device manufacturers, and EHRs. Members of the Workstream also developed a matrix that identified the risks, gaps, challenges, and best practices.

Appendix C. Task Force Meeting Agendas and Speakers

This appendix lists all public and private session HCIC Task Force meetings and associated agendas. Briefings included a wide range of topics to assist the Task Force in addressing its charge under CISA and developing this report and associated recommendations.

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

Wednesday, May 16, 2016 – Teleconference and HHS – Washington, DC
Welcome and Introductions • Kathryn Mart – Counselor to the Secretary for Health Policy, HHS
Introduction of HCIC Task Force Members • Steve Curren – Director, Division of Resilience, ASPR, HHS
CISA Overview • Emery Csulak – CISO, CMS, Task Force Co-Chair
HCIC Task Force Member Selection Process • Emery Csulak – CISO, CMS, Task Force Co-Chair
HCIC Task Force Structure, Operations, and Requirements • Emery Csulak – CISO, CMS, Task Force Co-Chair
Meeting Cadence and Logistical Items • Emery Csulak – CISO, CMS, Task Force Co-Chair

Thursday, April 21, 2016 – United States Access Board, Washington, DC
Welcome and Introductions • Mary K. Wakefield, Ph.D. – Acting Deputy Secretary, HHS
Health Care Industry Cybersecurity Task Force Overview • Emery Csulak – CISO, CMS and Task Force Co-Chair • Theresa Meadows – Senior Vice President and CIO, Cook Children's Health Care System and Task Force Co-Chair
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
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
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 ISAC
Discussion and Review of Open Session
Discussion of Potential Task Force Activities and Products
Discussion of Media Engagement
Planning for Subsequent Task Force Meetings and Next Steps

Thursday, May 19, 2016 – Teleconference and HHS – Washington, DC
Questions & Feedback: April 2016 Task Force Meeting
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
July 21 Meeting Planning
Logistical Updates

Thursday, June 16, 2016 – Teleconference and HHS – Washington, DC
Review: Draft Deliverable Framework
Discussion of Framework
Discussion of Workstreams
July 21 Meeting Planning
Administrative Items

Thursday, July 21, 2016 – Deloitte, Arlington, VA
Welcome and Introductions
Table Talks
Discussion of Framework Findings from Table Talks
Task Force Progress Review
Cybersecurity Best Practices – Finance and Healthcare ISAC Sector Panel • Jim Routh – Chief Security Officer, Vice President, Aetna Inc.
Discussion of Medical Device Workshop – 2 Day Workshop Out brief • Aftin Ross, PhD – Senior Project Manager, FDA
Task Force Progress Out Brief
CYBERSTORM5 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 Ecosystem • Margie Zuk, MS – Senior Principal Cybersecurity Engineer, MITRE Corporation
Planning for Subsequent Task Force Meetings and Next Steps

Thursday, August 18, 2016 – Teleconference and HHS – Washington, DC
Questions & Feedback: July 2016 Task Force Meeting
Review Provided Materials from July Meeting
Task Force Workstream Out-Briefs
Review: Framework
Discussion of CISA Sub-Sections D and E
Administrative Items

Thursday, September 15, 2016 – Teleconference and HHS – Washington, DC
Questions & Feedback: August 2016 Task Force Meeting
Task Force Workstream Out-Briefs
Review Report Examples and Draft Report Outline
Administrative Items

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
Panel Discussion: The Federal Approach for Health Care Industry Cybersecurity • Leo Scanlon – Acting CISO, HHS • Iliana Peters – Senior Advisor for HIPAA Compliance and Enforcement, Office for Civil Rights, HHS • Lucia Savage – Chief Privacy Officer, Office of the National Coordinator for Health Information Technology, HHS • Steve Curren – Director, Division of Resilience, ASPR, HHS • Suzanne Schwartz, MD – CDRH Associate Director for Science and Strategic Partnerships, FDA • Theresa Meadows (Moderator) – Senior Vice President and CIO, Cook Children's Health Care System and Task Force Co-Chair
Panel Discussion: Commercial Sector Information Sharing • Matt Hartley – Vice President Intel Operations & Products, FireEye • Anna Turman – CIO, 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, HITRUST • Terry Rice – NH-ISAC Board of Directors Member, and Vice President IT Risk Management and Chief Information Security Officer, 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, HITRUST
CHIME Survey Results Discussion

• Mari Savickis – Vice President, Federal Affairs, College of Healthcare Information Management Executives
Task Force Workstream Out-Briefs
Break Out Groups
Logistics for Thursday Working Session
Task Force Working Session
Task Force Next Steps and Developing the Report to Congress

Thursday, November 17, 2016 – Teleconference and HHS – Washington, DC
Questions & Feedback: October 2016 Task Force Meeting
Task Force Workstream Out-Briefs
Round Robin: Top 3 Concerns for the Health Care Industry
Health Care Industry Specific Break-Out Discussion
Recommendations Development and Follow-Up
Administrative Items

Wednesday, December 14, 2016 – DHS, Arlington, VA **Thursday, December 15, 2016 – Deloitte, Arlington, VA**
Opening Remarks
Report 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
Administrative Items
Task Force Working Session
HIMSS EHR Association Discussion • Justin Armstrong – MEDITECH, Privacy and Security Workgroup • Ross Berning – Epic, Privacy and Security Workgroup • Ann Marie Dunn – MEDITECH, Privacy and Security Workgroup • Isis Estevez – 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, MBA – CDRH Associate Director for Science and Strategic Partnerships, FDA

Task Force Working Session

Educational Resources for the Health Care Industry

- Margie Zuk – Senior Principle Engineer, MITRE
- Penny Chase – Senior Principle Scientist, MITRE

America's Health Insurance Plans (AHIP) Presentation

- Marilyn Zigmund Luke – Vice President, Special Projects, Executive Office, AHIP

Healthcare Information and Management Systems Society (HIMSS) Presentation

- Jeff Coughlin – Senior Director, Federal and State Affairs, HIMSS

Medical Device Innovation, Safety and Security Consortium Discussion

- Dale Nordenberg, MD – Chief Executive Officer, Novasano Health and Science

Closing Remarks

Thursday, January 12, 2017 – Teleconference and HHS – Washington, DC

DHS Cybersecurity R&D Initiatives Discussion

- Dr. Dan Massey – Program Manager, Cyber Security Division for the Homeland Security Advanced Research Projects Agency, DHS

HIMSS Cybersecurity Data Discussion

- Lee Kim, JC – 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

Thursday, January 17, 2017 – Teleconference and HHS – Washington, DC
Review: Draft Deliverable Framework
Administrative Items

Thursday, February 9, 2017 – Teleconference and HHS – Washington, DC

Monday, February 20, 2017 – Teleconference and HIMSS Conference – Orlando, FL

Appendix D. Cybersecurity Best Practices from Other Critical Infrastructure Sectors

To address subsection A of CISA section 405 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 and information from members of the Financial Services, Energy, and Banking 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.

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 HPH, Financial Services struggles with scaling for size to reach small businesses, 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 powerfully shape the cybersecurity risks of the sector. These risks reflect the nexus 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.[49] 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 hacktivists who are politically motivated.

Like the HPH Sector, the Financial Services faces serious issues with the error category of threat action. In both sectors, adversaries often exploit misconfigured or unpatched systems in order to conduct cyber attacks. The Financial Services Sector 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. [50]

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

[49] New York State Department of Financial Services. (2014, May). *Report on Cybersecurity in the Banking Sector*. Retrieved from: https://cybersecuritylawandpolicy.files.wordpress.com/2014/05/new-york-state-department-of-financial-services-report-on-cyber-security-in-the-banking-sector.pdf

[50] Vijayan, J. (2015, June). *Security Spending and Preparedness in the Financial Sector: A SANS Survey*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032

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.[51] 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 have broadly apply five key areas to address cybersecurity-related challenges. The table below summarizes key statistics and findings for each sector:

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 ensure the management of 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.
Information Sharing Organizations	Cybersecurity requires ongoing coordination and collaboration between those who experience threats and those who design and implement solutions. Information	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 ISAC serves as the largest source of	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

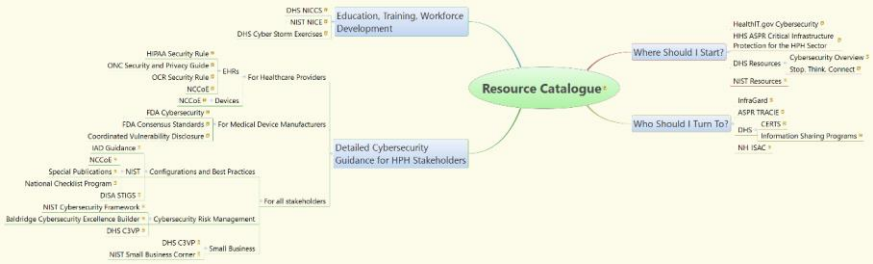
[51] CISCO. (2016). *Utility and Energy Security: Responding to Evolving Threats*. Retrieved from: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/security-benchmark-study-utilities.pdf

Best Practice	Why is it Helpful?	Financial Services Sector	Energy Sector
	sharing is crucial to increase threat awareness and mitigate overall risks.	information for the sector by providing resources from the government, subscription feeds, information from member companies and other ISACs. The ISAC 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.	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 or 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 detect cyber threats and vulnerabilities.	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 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.	60 percent of institutions conduct a regular security assessment or audit in order to better understand the status of and protect control systems.
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.	A majority of the broker-dealers (84 percent) and approximately a third of the advisers (32 percent) 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 or not vetting third parties.

Additionally, subject matter experts from the Financial Services and Energy Sectors identified the following leading practices to preventing and managing 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, but also 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. Resource Catalog



1. Where Should I Start?

HHS Resources

HealthIT.gov Cybersecurity: HHS Office of the National Coordinator for Health IT (ONC), has developed resources for healthcare cybersecurity and risk management. The HealthIT.gov Cybersecurity website points to these resources, including the Top Ten Tips and cybersecurity training games.

https://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility

HHS ASPR Critical Infrastructure Protection for the HPH Sector: HHS Assistant Secretary for Preparedness and Response's (ASPR) website on Critical Infrastructure Protection for the HPH sector includes cybersecurity resources, including the Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101 and a Cybersecurity Checklist.

https://www.phe.gov/Preparedness/planning/cip/Pages/protect.aspx

DHS Resources

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

https://www.dhs.gov/topic/cybersecurity

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.

https://www.dhs.gov/stopthinkconnect

NIST Resources

The National Institute of Standards and Technology (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.

https://www.nist.gov/topics/cybersecurity

2. Who Should I Turn To?

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

https://www.infragard.org/

ASPR TRACIE: ASPR's Technical Resources, Assistance Center, and Information Exchange (TRACIE) was created to meet the information and technical assistance needs of regional ASPR staff, healthcare coalitions, healthcare entities, healthcare providers, emergency managers, public health practitioners, and others working in disaster medicine, healthcare 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, ensuring patient safety and operational continuity.

https://asprtracie.hhs.gov/technical-resources/86/Cybersecurity/86

DHS

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

https://www.us-cert.gov/

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, including medical devices.

https://ics-cert.us-cert.gov/

Information Sharing Programs: This is the landing page for DHS's various programs for sharing cybersecurity information with private industry, including Automated Indicator Sharing

(AIS), Cyber Information Sharing and Collaboration Program (CISCP), Enhanced Cybersecurity Services (ECS), ISAOs, and the NCCIC.

https://www.dhs.gov/topic/cybersecurity-information-sharing

NH-ISAC

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

https://nhisac.org

3. Detailed Cybersecurity Guidance for HPH Stakeholders

For Healthcare Providers - EHRs

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

http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

ONC Security and Privacy Guide: The Office of the National Coordinator for Health Information Technology (ONC), in coordination with the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) created a guide to privacy and security of electronic health information, along with a Security Risk Assessment Tool.

https://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information

OCR Security Rule: The HHS Office of Civil Rights (OCR) has 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.

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

NCCoE: One of the NCCoE Health IT projects is EHRs on Mobile Devices.

https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices

For Healthcare Providers - Devices

NCCoE: One of the NCCoE Health IT projects is Wireless Infusion Pumps.

https://nccoe.nist.gov/projects/use_cases/medical_devices

For Medical Device Manufacturers

FDA Cybersecurity: FDA's Cybersecurity web page summarizes FDA's activities related to medical device cybersecurity, including issuing pre-market and post-market guidance, issuing Safety Communications for vulnerabilities discovered in devices, convening public workshops, and entering into a Memorandum of Understanding with the NH-ISAC and MDISS.

http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

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

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfstandards/textsearch.cfm

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

http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

For all stakeholders – Configurations and Best Practices

IAD Guidance: Information Assurance at NSA 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.

https://www.iad.gov/iad/library/ia-guidance/index.cfm

NIST NCCoE: The NIST National Cybersecurity Center of Excellence (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 SP 1800 series).

https://nccoe.nist.gov

NIST Special Publications: The NIST Special Publications 800 series provides computer/cyber/information security guidelines, recommendations, and reference material. Special Publication 800-53 is the core guide for assessing security and privacy controls 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 a wide range of technologies (e.g., servers, mobile devices, cloud computing, encryption, and wireless protocols).

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

http://csrc.nist.gov/publications/PubsSPs.html

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.

https://web.nvd.nist.gov/view/ncp/repository

DISA STIGS: The Defense Information Systems Agency (DISA) publishes the Security Technical Implementation Guides (STIGs), which provide configuration guidance for information assurance enabled DoD systems. Even though these STIGS provide configurations for DoD systems, manufacturers and healthcare 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.

http://iase.disa.mil/stigs/Pages/a-z.aspx

For all stakeholders – Cybersecurity Risk Management

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.

https://www.nist.gov/cyberframework

Baldridge Cybersecurity Excellence Builder: NIST's Baldridge 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 Baldridge Excellence Framework with the concepts of the CSF.

https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

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

The C3VP website contains information about the CSF, 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.

https://www.us-cert.gov/ccubedvp

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.

https://www.us-cert.gov/ccubedvp/smb

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 SBC Library contains workshop materials and a link to NISTIR 7621 r1: Small Business Information Security: The Fundamentals.

http://csrc.nist.gov/groups/SMA/sbc/

4. Education, Training, Workforce Development

DHS NICCS: DHS's National Initiative for Cybersecurity Careers and Studies (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 NSA, K-12 resources, and industry resources.

https://niccs.us-cert.gov/cybersecurity

NIST NICE: NIST's National Initiative for Cybersecurity Education (NICS) 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 Framework, a taxonomy for classifying cybersecurity roles), educational activities and programs, and other materials and resources that support cybersecurity training.

https://niccs.us-cert.gov/cybersecurity

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 healthcare and public health sector.

Appendix F. Health Care Subsector Risks across the Value Chain

The following table documents some risks identified by organizations representing pharmaceuticals, health plans and payers, medical devices and equipment, laboratories and patient service centers, providers, and health information and medical technology across the health care value chain.

	Confidentiality	Availability	Integrity	Patient Safety
R&D	Theft of non-patented intellectual property or other proprietary information Exposure of PHI Exposure of clinical trial data Exposure of information or insider trading on licensing or merger and acquisition activities	Loss of adverse event/safety reporting system hinders timely reporting of safety issues	Modifications to (or of) clinical trial results and data sets resulting in corrupted data sets or fraud	Privacy and security aspects not include in the original design
Manufacturing	Theft of trade secrets related to manufacturing processes or SCADA system settings in biologics arena	Disruption of supply chain (incipient and active pharmaceutical ingredients) Disruption of supply chain or major facility impact	Manipulation or corruption of systems or data related to validated processes and systems Improperly managing validated system lifecycle (i.e., patching, EOL status, vendor support, etc.)	Improper dosing or combination of ingredients Quality issues related to device manufacturing
Supply Chain	Hardware or software may have intentional or unintentional vulnerabilities	Software or hardware may or may not be reliable	Software or hardware errors may introduce integrity problems	Manipulation of patient application leads to

	Confidentiality	Availability	Integrity	Patient Safety
	that can be exploited for unauthorized disclosure of information Hardware or software may not be designed with security in mind (e.g., no threat modeling) Exposure of credit card data Exposure of customer, patient, or physician personal data	Denial of service attacks may result from software bugs Distributed denial of service attacks would impact sales sites and purchasing portals	Manipulation or alteration of sales or distribution data	improper usage of medication Insecure supply chain data related to product distribution or therapy availability
Corporate Functions	Exposure of earnings reports prior to public disclosure Reputational impact/ consequences from data breach Provider financial data linked to PHI and demographics	Inability to meet Securities and Exchange Commission and regulatory reporting timelines	Manipulation or corruption of systems/data related to finance, quality, regulatory, or clinical functions	
Medical Devices and Equipment	Medical device, application, and/or underlying systems or databases are exploited and/or infected with malware/virus leading to unauthorized access to and/or theft of data Imaging systems and radiation medicine include PHI and patient identifiers	Medical device, application, and/or underlying systems or databases are exploited and/or infected with malware/virus making device (and possibly other parts of network) unavailable	Medical device, application, and/or underlying systems or databases are exploited leading to compromise of other systems or other parts of network Medical device, application, and/or underlying systems or	Patient safety may be jeopardized by delaying or preventing diagnostic testing from being performed Patient safety may be jeopardized by delivering an incorrect dosage of if hacked

	Confidentiality	Availability	Integrity	Patient Safety
		Pumps, implantable devices, and others may be wireless and can be hacked or altered Video monitoring could be hacked (challenge especially for behavioral health units)	databases are compromised leading to specimen/patient data being altered or deleted Incorrect testing ordered and patient data could be altered (imaging systems and radiation medicine)	
EHR	Compromise of EHRs could expose patient PHI	Physicians and providers are dependent on EHRs for patient information	Compromise of EHRs could result in the theft or alteration of patient data Compromise of EHRs could result in the ability to alter orders	
Diagnostic Specimen Testing	Systems, phlebotomist workstations, and/or applications used to record receipt of specimen information is compromised, resulting in stolen test results, specimen data, patient data, or physician information Systems used to record, store, and distribute test results is compromised, resulting in stolen test results or specimen data	Systems used to record receipt of specimens and process specimens is subject to distributed denial of service attacks or otherwise compromised and unavailable Phlebotomist workstation is exploited rendering workstation unavailable for use Systems used to record, store, and distribute test	Systems used to record receipt of specimens; process specimens; and record, store, and distribute test results is compromised, resulting in: • Alteration of specimen, test results, or patient data • Inaccurate, incomplete, and/or mislabeled	Patient health could be jeopardized by: • Requiring resampling specimen from patient • Delaying or preventing diagnostic testing from being performed • Reporting inaccurate and/or incomplete test results

	Confidentiality	Availability	Integrity	Patient Safety
		results is subject to distributed denial of service attacks or otherwise compromised and unavailable preventing test results from being sent (to physicians and/or patients directly)	instructions for specimen processing • Stolen test results • Inaccurate instructions for processing • Test results sent to the wrong patient or physician	• Not reporting test results or not reporting in a timely manner
Legacy Systems		Multiple small programs throughout which are probably without security updates		
Pharmacy	Compromise of pharmacies could expose patient PHI	Pharmacies are dependent on EHRs for information	Compromise of pharmacies could result in the theft or alteration of patient data Compromise of pharmacies could result in the ability to alter orders	Compromise of pharmacies could put the patient at risk due to incorrect medications or dosing
Provider and Office Support Systems	Exposure of credit card data through point-of-sale system Exposure of customer/ physician personal data Providers that only use user IDs & passwords are susceptible to having			

	Confidentiality	Availability	Integrity	Patient Safety
	credentials stolen & unauthorized access Need for multi-factor authentication that is seamless with user workflow (with second factor being out-of-band) Medical staff database for credentialing contains demographics Medical staff database for credentialing contains confidential personal information (as do HR files) Registration system contains demographic data – links to HER and all medical records. Critical to patient identification as well as financial impact for billing ADT system is usually linked to all other systems			
Patient Portal	Access to medical records and ability to interact with providers is another access point for entry			
Governance & Oversight	Not enforcing security policies or a lack of accountability leads to	Uncontrolled risks may lead to a lack of resource availability	Uncontrolled risks may lead to a lack of resource integrity	

	Confidentiality	Availability	Integrity	Patient Safety
	inconsistent governance and ineffective policies Need for top-down approach to governance, policies, and risk management with a "whole of organization" approach Need for oversight at all levels and enforcement so that one has accountability re: security policies Need for better coordination between Human Resources and IT re: timely provisioning & de-provisioning of accounts (especially the latter may lead to unauthorized access & breach of data) Need for oversight with regard to workforce members & third party vendors & consultants (not set it and forget it, but rather monitoring the performance and assuring adherence to the organization's security policies during the business relationship)	Risk of logic bombs, wiper malware, etc.		

	Confidentiality	Availability	Integrity	Patient Safety
	Need for business continuity & disaster recovery re: manmade & natural disasters & incidents with regard to health IT assets			
Endpoint Security; Physical Security; Network Security; Mobile Security	Endpoint security: Need for host-based solutions; layered solutions with defense in depth; need for link encryption and whole disk encryption, encrypted media, etc. Physical security: Need for safeguarding of equipment & data; physical access to equipment or data can defeat technical controls; lack of stringent policies re: facility controls and building access Network security: Need for segmenting networks; commingling of information can lead to compromise of information; also, need for mitigation re: ARP cache & DNS poisoning Mobile security: need for link encryption (especially over insecure lines, such as WiFi & cellular networks);	Ransomware encrypts data and filenames Denial of service caused by an attacker or a bug (need for network & CPU load balancing)	Ransomware Risk of information being tampered with or corrupted in transit (need to encrypt and hash information)	

	Confidentiality	Availability	Integrity	Patient Safety
	need for mobile device management			
Health Plans and Payers	Social security number, PHI, or patient demographics leakage SSN leakage through email and file transfer Phishing Fraudulent claims Health provider visits	Social security number or PHI leakage Denial of service attacks on the web portal Mishandling of sensitive information by the provider	Fraudulent claims Pharmacy SPAM & fraud Voice fraud Provider system breach	Content scraping and botnets Phishing of doctor's office
Third Party Vendors and Consultants	Backdoors written into software (or hardware) Buffer overflow errors in software (or hardware) Insider threat (negligent and malicious) Failure to limit privileges/access to least privilege & need to know (should use a DMZ to limit access & least privilege) Lack of penetration testing and security testing (overall) with vendor solutions before "go live" (full production) Often linked electronically	Resources not being available (e.g., cloud service or other third party service); unexpected, unscheduled downtime	Insider threat (negligent and malicious)	Any compromise of C,I, and/or A can adversely affect patient safety

	Confidentiality	Availability	Integrity	Patient Safety
	Can act as an entry point to IT systems			