2-25-2020

Maybe If We Turn It Off and Then Turn It Back On Again? Exploring Health Care Reform as a Means to Curb Cyber Attacks

Deborah Farringer
Belmont University College of Law

Maybe If We Turn It Off and Then Turn It Back On Again? Exploring Health Care Reform as a Means to Curb Cyber Attacks

Deborah R. Farringer

Introduction

In this digital age, hardly a day goes by without a story in the news about identity theft,[1] a ransomware attack,[2] a data breach exposing personal data,[3] or other instance in which electronic information is unintendedly or deliberately disclosed to third parties.[4] While these cyber-related events have become increasingly common, the movement towards electronic storage of information and electronic transactions and communication has continued unabated because the benefits of electronic communication tools exceed the associated risks.[5] The health care industry is no exception. It has moved at a rapid pace away from paper records to an electronic platform across almost all sectors — much of it at the encouragement and insistence of the federal government.[6] Such rapid expansion, however, has increased exponentially the risk to individuals. This risk is not simply financial or reputational to the extent that sensitive patient data is exposed to third parties, but also has become increasingly a risk to an individual's physical safety when medical records are inaccessible to providers or when attackers tamper with records data or medical device use or data.[7]

Globally, the health care industry is in the bottom third of industries when it comes to frequency of breaches,[8] but certain unique challenges make it a leader in other categories.[9] For example, in 2018, the average per capita cost of a data breach for the health care industry globally was $408,[10] which was over $200 higher than the cost experienced by the next closest sector — the Financial sector — and nearly three times the global average per capita cost of $148.[11] There are a number of factors that contribute to this figure. First, the health care industry has an unusually high churn rate due to the multitude of electronic health record ("EHR") vendors.[12] Also, unlike most other industries, the health care industry and its various sectors are regulated and managed by multiple federal and state agencies that each have some level of oversight or jurisdiction over certain aspects of the industry, making it difficult for those in the industry to adopt a coordinated and cohesive approach to cybersecurity.[13]

Consequently, when the United States Congress took action to increase cybersecurity across the nation under the Cybersecurity Information Sharing Act of 2015 (CISA), it recognized the health care industry required a different approach.[14] Through this law, Congress established the Health Care Industry Cybersecurity Task Force ("Task Force") for the purpose of reviewing cybersecurity risks within the health care industry and identifying who will lead and coordinate efforts to address such risks among the various agencies.[15] The Task Force issued a report in June of 2017 (the "Report"),[16] setting forth six high-level imperatives that the health care industry needs to achieve in order to combat cybersecurity, each accomplished through multiple recommendations and action items.[17] Notably, many of the vulnerabilities plaguing the industry that are identified in the Report as requiring correction are not necessarily related to specific flaws in the current cybersecurity framework, but rather susceptibilities presented by the infrastructure and associated regulatory regime that has evolved over the last few decades over the health care industry generally.[18] That is, the current health care infrastructure by its nature exacerbates cybersecurity risk. Among these infrastructure obstacles, the Task Force noted that a

Deborah R. Farringer, J.D., *is the Director of Health Law Studies and an Associate Professor at Belmont University College of Law. Her scholarship explores the operation and impact of health laws and health policy on providers and suppliers.*

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)
DOI: 10.1177/1073110519898046

lack of information sharing of industry threats, risks, and mitigations,[19] disparate leadership and governance goals for cybersecurity,[20] and the confluence and contradiction of existing federal and state laws that have all led to heightened cyber risk for the health care industry.[21] Further, operational system challenges such as fragmentation in the current fee-for-service delivery system and its resulting lack of care coordination, disparate attention-span of various industry participants — especially providers — for implementation of cybersecurity initiatives, and lack of available resources across and among sectors to promote cybersecurity as a priority all threaten cybersecurity.[22] Solutions that are reactive to problems within the current infrastructure will likely have little long term impact toward reducing cybersecurity vulnerabilities because they do not address the underlying system challenges. The Task Force acknowledges these challenges, and, at times, avers that the certain recommendations might need to be transformative to the system,[23] but falls short of suggesting more comprehensive reform as a means to address cybersecurity risk.[24] Still, the question remains: if in fact the current health care delivery infrastructure is a contributing factor to the incidents of cybersecurity attacks and the exorbitant costs associated with resolving data breaches, should Congress look not just to curb breach incidents, but to address root cause systematic challenges in the health industry infrastructure that create increased exposure of cybersecurity threats?

Exploring this question, in Part I, the article examines the current cybersecurity crisis and what efforts have been made thus far to address and defend against existing known cybersecurity threats. Part II analyzes the specific recommendations set forth by the Task Force to identify certain themes that have emerged regarding systematic challenges that are counter indicated for curbing cyber risks and explores infrastructure reform initiatives to analyze how such programs could aid in curbing cyberattacks. In Part III, this article argues that cybersecurity risks will continue to be heightened and more costly to the health care industry as compared to other industries unless and until some general system redesign is achieved that allows for (1) greater sharing of resources among industry participants to ensure the same protections are implemented at all levels of the industry, which can be strengthened through greater interoperability of systems across the health care industry;[25] and (2) increased focus and attention on the importance of cybersecurity issues as a priority among system reforms. Finally, Part IV concludes by offering some suggestions and recommendations for which system redesigns should lead the way that will most effectively put the health care industry in the best possible position to mitigate cybersecurity risk.

I. Background

While the push toward EHRs was perhaps officially spurred with the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[26] it has taken the health care industry a number of years and different legislative efforts to achieve more widespread EHR adoption.[27] Finally, following enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, health care providers undertook rapid and widespread adoption of EHR systems.[28] By 2017, nearly eighty-six percent (86%) of physicians used an EHR system (with just over seventy-nine percent (79%) using a certified EHR system),[29] and ninety-six percent (96%) of all hospitals possessed a certified EHR system.[30]

[If] in fact the current health care delivery infrastructure is a contributing factor to the incidents of cybersecurity attacks and the exorbitant costs associated with resolving data breaches, should Congress look not just to curb breach incidents, but to address root cause systematic challenges in the health industry infrastructure that create increased exposure of cybersecurity threats?

While more comprehensive use of EHRs across various providers has had certain positive impacts on health care services and quality care through a decrease in prescribing errors, reduction of duplication of services, compliance with standards of care, and improvement of patient safety,[31] the transition to an electronic format has been challenging and not without controversy.[32] Certainly, regulators anticipated the need for increased privacy and security measures once data was transferred into an electronic format and more widely shared among providers and suppliers, as evidenced by enactment of HIPAA and its privacy and security regulations.[33] But, the modern day sophistication and skill of internet hackers and

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

other cyber criminals and associated tactics could not yet have been imagined.[34] Thus, while the health care industry and its patients are by now well trained on standard HIPAA privacy protections, many providers remain unaware or unprepared for more comprehensive cybersecurity risks posed by deliberate third party actors.[35]

Certainly, the health care industry has not been alone in facing a frightening new reality of cyber-espionage and theft of intellectual property, trade secrets, and government information.[36] Noting an 1100% increase in incidents of loss, theft, and exposure of personally identifiable information from 2006 to 2015,[37] U.S. Congress reacted to this new threat by enacting the CISA.[38] The CISA established the Task Force and tasked it to to address cybersecurity in the unique setting of the health care industry in the form of six tasks.[39] The Task Force issued six imperatives and related recommendations and action items.[40] Noting the challenges in attempting to create uniform recommendations for an industry described as a "mosaic,"[41] the Task Force identified three major risk areas across the industry.[42] First, it noted that there is a distribution of different types of risks across the health care value chain in the context of cybersecurity, which includes risk to: the confidentiality of medical records data; the availability of the data; the integrity of the data; and patient safety.[43] Further, these risks vary across the numerous sectors that comprise the health care industry.[44] For example, the greatest cybersecurity risk to a healthcare provider in the provider's daily practice might be of little to no risk to an equipment manufacturer. Ensuring protection of each part of the EHR system, however, is critical to the protection of the system as a whole.[45] Second, the Task Force considered risks to EHRs specifically and noted that while lack of interoperability is one of the obstacles that creates the greatest risk to achieving cybersecurity, interoperability through a "shared, publicly-available application interface could expose EHRs to additional attack vectors."[46] Thus, any potential solutions or a regulatory framework designed to establish interoperability must be developed with these increased risks in mind.[47] Interoperability and how to achieve it has been a particularly vexing issue over the years, as a number of initiatives for health information exchanges have been attempted, but few successes have been realized in achieving wide-spread use or adoption.[48] Achieving greater data sharing while simultaneously protecting this now consolidated data remains a key area of concern. Lastly, the Task Force considered risks posed through medical devices, software, and other connected devices that are not themselves a medical record, but compromise the integrity of the whole because of the connectedness to an EHR network more generally.[49]

Acknowledging these differing risks and having established the lens through which the Task Force worked in trying to consider the best approach for cybersecurity, the Task Force provided recommendations and action items both specific to particular sectors or devices and broadly directed to the industry more generally.[50] The breadth and depth of the recommendations and action items demonstrate how challenging mitigating cyber risk is and will continue to be in the health care setting.[51] As contrasted by HIPAA statutes and regulations, the imperatives encompass confidentiality and security related to the maintenance of such confidentiality, along with the competing concerns of access to information, integrity of information, and related potential harm to patients if the information is either inaccessible or compromised.[52] Thus, the Report considers numerous ways in which the industry is vulnerable to cyber threats and addresses each particular threat, presenting action items for how each could be remedied or approached.[53] The Task Force concedes that its structure could encourage industry participants to implement only such action items that pertain to one's specific needs.[54] The Task Force warns against adopting only some of the action items, however, because it will not likely achieve the same benefits and will not "maximize [one's] financial investments and personnel resources."[55]

In the two years since the issuance of the Report, Congress has taken additional legislative action to address some of the specific challenges of interoperability and connectivity.[56] The 21st Century Cures Act (the "Cures Act"),[57] enacted in 2016,[58] seeks to promote(s) nationwide interoperability that thus far has been plagued by "deficits in trust between organizations and by anti-competitive behavior that results in the holding of patient [electronic health information]"[59] and by the sheer number of EHR vendors that exist, each on different platforms and designed for different specialties.[60] The Cures Act requires the Office of the National Coordinator for Health Information Technology (ONC) to "defin[e] the requirement for health IT developers of certified health IT to publish application programming interfaces (APIs) that can be used 'without special effort' to drive individual, clinician, and payer access to clinical data; and [to develop] a comprehensive approach to address information blocking."[61] Further, the Cures Act directs the ONC to "develop or support a trusted exchange framework, including a common agreement among health information networks (HINs) nationally."[62] The ONC has released two drafts of the Trusted Exchange Framework and Common Agreement, which endeavor

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

to create the necessary rules and regulations for sharing electronic health information across networks and develop a governance structure that can eventually spur interoperability between disparate networks to increase quality care and patient safety.[63] While the ONC acknowledges the need for HINs to establish baseline privacy and security requirements as required by HIPAA, the Common Agreement does not utilize HIPAA requirements as a baseline.[64]

It cannot be overstated that interoperability poses its own unique set of challenges, including the fact that one effect of interoperability is greater amounts of data consolidated into one place.[65] Certainly, this is a reason to be both cautious and thoughtful when considering implementation and infrastructure of interoperability. While these concerns remain, the Task Force recognizes that increased interoperability and promotion of a common security framework can have a positive impact on curbing cyberattacks[66] and as progress towards achievement of its ultimate goals.[67]

In addition to interoperability, the Task Force has reported some progress in each of the six imperatives, ranging from development or participation on certain committees to the creation of educational and resource materials to inform the industry about the need for action and diligence.[68] As with the imperatives themselves and the impacts of the associated action items, progress has been variable across sectors,[69] but no changes have been able to fundamentally transform cybersecurity wholesale.[70] Thus, various sectors of the industry are taking action on certain items, but widespread movement towards an industry-wide effort to tackle common and complex security issues remains stagnant. It is not surprising that early efforts have concentrated primarily on educational efforts, as the Task Force recognizes that one of the biggest challenges to addressing cybersecurity will be mitigating the current fatigue that many providers in the industry are already feeling with the move into the digital space.[71]

II. Structural Challenges to Cybersecurity Recommendations

The Report has elicited certain themes regarding the key structural challenges that exist within the health care industry that make addressing cybersecurity risks especially difficult.[72] First, the size and structure of the various organizations that comprise the health care industry across all of its sectors are hugely diverse, which often results in a disparity of resources to implement system-wide change.[73] This structural reality creates implementation barriers across a number of different imperatives and recommendations.[74] Although diversity of size, scale, and scope by itself is not necessarily a detriment to the patient-level delivery of health care services[75] or to the provision of quality care, it does create a significant incongruence in how differing components of the health care industry — even within sectors — are reacting and responding to cybersecurity risks.[76] Thus, while large systems might have the resources, infrastructure, governance support, and personnel to implement the necessary tools to be prepared for a cyberattack, a small physician practice might have limited resources and little motivation to dedicate hard-earned practice dollars to security for EHRs.[77] Similarly, large-scale medical device manufacturers might have an entire team of people focused on ongoing data security and protection, whereas a small manufacturer might have limited resources beyond basic production and maintenance.[78] This resource disparity is not an issue that is easily addressed at the sector-level or at the industry-level given that the dichotomy of organizational size and financial capabilities is at least in some part a product of the existing legal framework that hinders consolidation and collaboration rather than encourages or promotes resource sharing.[79] That said, even when legal waivers have been granted to try and ease these regulatory burdens, moving into a new and different payment structure has been difficult and challenging.[80]

Second, the existing regulatory scheme that governs the health care industry, including the Affordable Care Act (ACA),[81] HIPAA, HITECH, the Physician Self-Referral Law (known as the "Stark Law"),[82] the Anti-kickback Statute (AKS),[83] the False Claims Act,[84] and various other state laws, provides significant barriers toward collaboration and interoperability. The Stark Law and the AKS often stand as obstacles toward the sharing of resources that could facilitate larger organizations assisting smaller organizations with technology and cybersecurity resource needs.[85] The Report stated: "We strongly encourage Congress to evaluate an amendment to [the Stark Law and the AKS] specifically for cybersecurity software that would allow health care organizations the ability to assist physicians in the acquisition of this technology, through either donation or subsidy."[86] It should be noted that CMS published a proposed rule for modernizing the Stark Law on October 17, 2019.[87] Included in the proposed rule is an amendment to the existing Stark Law exception that would clarify the requirement regarding interoperability, prohibit information blocking and data locking, and further include software and hardware that is not only related to the EHR itself but is instead for cybersecurity purposes to "protect" EHRs.[88] CMS is seeking comments about whether to make the exception permanent or extend the current timeline, which contemplates the exception sunsetting after a time.[89]

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

Although certain exceptions and safe harbors exist that provide health care organizations with some protections, those exceptions and safe harbors do not go far enough to assist with expenses and resource needs that extend beyond an initial purchase or implementation.[90] Additionally, some organizations are bound by state laws that apply similar restrictions as those imposed at the federal level.[91] Moreover, even if hardware and software challenges are addressed under applicable exceptions and safe harbors, other federal laws such as HIPAA and HITECH create data sharing barriers.[92] Indeed, the Task Force noted that even the threat of breaches and penalties, fines and public disclosure can chill an organization from sharing information with other providers.[93] While the ACA created some avenues for greater collaboration and data sharing,[94] programs such as the Medicare Shared Savings Program do not act as a complete waiver of existing constraints under the Stark Law, the AKS, the False Claims Act, and applicable antitrust law; rather these laws impose other obligations and requirements that have made widespread provider adoption incongruent.[95] Because mitigating cybersecurity risk is premised at least in part on the ability to share information and anticipate new attacks, the complicated and web-like regulatory structure remains a challenge for the industry, especially providers.

A third theme emerging from the Report is the challenges posed by the continued lack of consistent and secure interoperability among and between systems, providers, medical devices, medication delivery systems, and other "Internet of Things" (IoT).[96] Granted, of those systematic challenges that complicate meaningfully addressing cybersecurity risk, interoperability seems to be the area with the most currently active and ongoing reform efforts.[97] Such reform efforts, however, have been inconsistent in their application, beginning with attempts to implement state-led health information exchanges before moving to a more federally-led effort as set forth under the Trusted Exchange Framework.[98] The convenience and advantages of connectivity among various medical devices and other technology, such as wearable technology or programmable pacemakers, is prompting such connectivity to take place prior to any comprehensive regulations or requirements.[99] Absent clear guidance regarding a specific infrastructure for interoperability, many data users, including providers and patients, are creating their own mechanisms for sharing data, not all of which may be as secure as would be required or recommended by industry guidance.[100]

Additionally, connecting all of the various sectors makes sense at the patient level, but the sectors themselves are not governed by the same agencies and therefore are subject to disparate rules and regulations.[101] For example, the federal Food & Drug Administration (FDA) has created guidance for Postmarket Management of Cybersecurity in Medical Devices to address some of these vulnerabilities, but the guidance is voluntary and addresses a portion of the "stakeholders," many of which are not regulated by the FDA.[102] Thus, although interoperability could address some cybersecurity concerns, connectivity without interoperability creates greater risk and vulnerabilities for the industry as a whole.[103] Achieving interoperability can actually mitigate known risks if it promotes large, resource heavy industry leaders to implement necessary controls across the continuum.

Finally, the fourth theme arising out of the Report regarding systematic obstacles relates to the myriad regulatory agencies that govern different aspects of the health care industry, which lack coordination and consistency in their approaches to cybersecurity risk mitigation.[104] Medical devices exemplify the quagmire that competing regulatory agencies create in the context of cybersecurity.[105] The FDA governs the manufacture and sale of medical devices, including the marketing of and the safety and efficacy of such devices.[106] Medical devices often times will contain personal health information, but manufacturers are not subject to HIPAA or the security regulations governing providers.[107] In contrast, the providers who use, install, and work with medical devices are subject to HIPAA for purposes of privacy and confidentiality of patient data, which is overseen by the Office for Civil Rights (OCR).[108] OCR imposes its own set of regulations and assesses applicable penalties for violations of HIPAA or HITECH regulations,[109] independent of other rules and regulations imposed by the CMS and enforced by the Office of Inspector General, and the Federal Trade Commission.[110] Yet, in order to mitigate cybersecurity risk, there needs to be a consistent approach among all components of an electronic health system, including medical devices, EHRs, medication delivery systems, and other IoT items. Although agencies have promoted industry participants to follow the National Insitute of Standards and Technology (NIST) standards, all such recommendations are voluntary and do not necessarily align with existing regulatory structures.[111]

Although some of the specific recommendations and action items can be accomplished, these four systematic issues seem to permeate through all of the six imperatives and impact the ability for the health care industry to focus its attention on specific cybersecurity issues such as preventing ransomware attacks or shoring up other EHR vulnerabilities. Unless and until there are changes to the health care infrastructure itself, there is a danger that entities will undertake

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

recommendations and action items that are the most easily accomplished, leaving some of the most vexing imperatives implemented only in part.[112] Unfortunately, this seems to be exactly what the Task Force was attempting to guard against when it stated that partial adoption of the recommendations and action items will not "maximize their financial investments and personnel resources."[113] Granted, wholesale adoption of all recommendations and action items will be challenging to achieve without comprehensive system reform.

not seek to address some of the interoperability and resource issues and help promote greater emphasis on the importance of cybersecurity efforts will do little to correct many of the systematic challenges mentioned above. The United Kingdom (U.K.)[116] provides a case study of this point: in 2018, the U.K.'s National Health Service (NHS) experienced a massive data breach when it was attacked by the "WannaCry hack," which shut down access to and demanded ransom payments from a third of hospital trusts in the U.K. and eight percent (8%) of primary care practices.[117] The attack

Many of the barriers to the industry, however, are not specific cybersecurity challenges, but are issues intertwined and endemic to the very nature of the current healthcare infrastructure. Therefore, while the Report is important work, it is insufficient to help fuel significant movement or change that will take adequate steps to enhance cybersecurity generally *until* more meaningful reform is enacted or implemented that addresses some of the systematic infrastructure issues that exacerbate cybersecurity risks.

III. Argument

What seems clear when considering these themes collectively is that identifying the structural issues that will create greater cybersecurity risk for the healthcare industry is a necessary first step because it narrows the scope of the types of reforms that will impact cyber risk. Many of the barriers to the industry, however, are not specific cybersecurity challenges, but are issues intertwined and endemic to the very nature of the current healthcare infrastructure. Therefore, while the Report is important work, it is insufficient to help fuel significant movement or change that will take adequate steps to enhance cybersecurity generally *until* more meaningful reform is enacted or implemented that addresses some of the systematic infrastructure issues that exacerbate cybersecurity risks.[114]

Health care "reform" has become a rather generic term, but can mean a number of different types of changes to healthcare delivery and payment mechanisms. Most, if not all, ongoing reform initiatives and current reform proposals address only some of the systematic barriers that complicate cybersecurity advancement. For example, so-called "Medicare for All" proposals that have been suggested by various Democratic candidates are largely focused on payment and access reform.[115] While these goals are laudable, when considering cybersecurity specifically, a single payor system or public option that does

was thought to have occurred due to the use by several hospital trusts and primary care practices of Windows XP, an operating system that dates back to 2001 and that Microsoft ceased to support in 2014.[118] While NHS provides health care services to any and all residents who need the services, similar to what is contemplated in a Medicare for All-type option, hospitals maintain their own systems and the U.K. has not yet transitioned to a common platform among all contracting providers.[119] Thus, even with adoption of a Medicare For All-like plan, the same cybersecurity challenges would remain absent a specific focus on interoperability and common infrastructure and shared platforms as part of reform efforts.

In contrast, while a single payor system or public option regime as currently contemplated would not address all infrastructure challenges that affect cybersecurity, these systems could lessen the chaos and confusion caused by the multiplicity of laws, regulations, and regulatory agencies governing the industry to the extent that the payment reform eliminated or reduced the need for certain legal hurdles. For example, enactment of the Stark Law and renewed enforcement of the AKS arose out of a fee-for-service payment structure that incentivizes volume of services and services reimbursed at the highest rate.[120] Adopting payment reform that shifts the focus away from fee-for-service — or at least away from medical decision making that

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

maximizes financial productivity as opposed to quality care — will reduce the need for application of laws that hinder collaboration or care coordination. Some of this payment reform has been ongoing through efforts to shift payment from volume-based to value-based — largely a focus on the twin goals of reducing cost and improving quality care in the form of enhanced outcomes.[121] These efforts promote care coordination and reduction in duplication of services and *could* help to enhance cybersecurity if achievement of such goals promotes collaboration and data sharing. For example, in a bundled payment model, providers will need to focus on assuring that the most cost efficient and effective provider is rendering the necessary medical care, which can be achieved through shared protocols and shared access to the medical record. A large hospital system that operates a sophisticated cybersecurity program[122] engaged in a bundled payment program with post-acute providers will likely require cybersecurity controls of the hospital to govern the data exchange, providing greater protection over devices, records, and other connected systems. Additionally, to the extent that collaborating systems begin to promote greater emphasis on cyber protections, sectors might also experience cultural shifts as more providers and suppliers begin to truly understand and appreciate the importance of cybersecurity.

Independent of infrastructure challenges, perhaps the biggest barrier to mitigating cyber risk is convincing individuals and entities to make the necessary investments to properly combat the known risks, which disproportionately impacts smaller and less-resource intensive entities.[123] Promoting programs such as accountable care organizations (ACOs),[124] clinically integrated networks (CINs),[125] and patient-centered medical homes that encourage larger, more financially stable entities to share resources with smaller, less financially stable entities,[126] will help spread cybersecurity resources to the most vulnerable areas.[127] A small physician office is unlikely to employ an IT professional whose sole focus is maintaining support for operating electronic systems and combating cyber threats,[128] but that same office as a participant in an ACO is able to utilize the resources within the ACO, facilitating better protection of all data contained within the system.[129] ACOs and CINs are incentivized and encouraged to engage in collaboration and care coordination to achieve cost savings, and these efforts are most easily accomplished through interoperability or other coordinated data sharing.[130] Because managing cyber risk becomes the responsibility of the ACO, resources toward this effort can be pooled and coordinated. Such coordination may also prevent churn and system migration of small providers, both of which make electronic systems more vulnerable to threats due to lack of support from fledgling vendors and compatibility barriers that prevent system integration and then increase breach costs as providers migrate to new vendors after each breach incident.[131]

ACOs, CINs, and like structures will also assist in moving more rapidly toward interoperability, as interoperability (done properly) will aid in achieving quality metrics and reduce expense through reduction of duplication of services.[132] The lack of interoperability in the current health care system has perpetuated make-shift data sharing mechanisms that are less secure and make data more vulnerable to cybersecurity risk.[133] Congress and CMS should move from voluntary recommendations for interoperability towards required security regulations and infrastructure standards. Such efforts will be easier to accomplish to the extent that resources can be allocated across the care continuum among larger and smaller actors in the market through reform efforts. Certainly, data breaches and cyberattacks will not be entirely prevented as a result of these incremental system reforms — such as ACOs and bundled payment models; however, the health care industry will be better poised and prepared to address and respond to attacks in a more efficient and less costly manner to the extent that this resource allocation can be spread across sectors.

Lastly, the confusion and chaos that is created by competing statutory and regulatory regimes and agencies remains a difficult issue to adequately address. There have been efforts by agencies to coordinate through deference to a common agency, such as recommendations to follow the NIST standards, or waivers of certain laws in lieu of others, such as waivers for ACOs under the ACA.[134] More coordination must take place, however. While agency consolidation or reconfiguration is unlikely, agencies could today mitigate existing barriers with promotion of increased coordination between agencies and adoption of regulations that apply across the industry. It is imperative in the context of cybersecurity that agencies engage in this coordinated effort because other initiatives to support care coordination will be thwarted to the extent that various sectors in the industry are forced to comply with disparate statutes, regulations, and directives.

Conclusion

Comprehensive health care reform that includes cybersecurity not just as a thought, but as a purpose and goal of system redesign would help to most efficiently and effectively address cybersecurity risk. While no singular current reform initiative particularly will address all of the structural challenges that exacerbate cybersecurity risk, many of the reform efforts, if

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

implemented and promoted, may make meaningful progress in the fight against cyber threats and cyber-attacks. Identifying applicable vulnerabilities is crucial, but it is clear through the Task Force's efforts that many of the challenges cannot be addressed piecemeal or only by market leaders. Rather, significant movement towards greater cybersecurity must begin with systematic infrastructure reforms that enhance, support, and promote collaboration, interoperability, and great sharing of resources. Although some current reform initiatives could be used for this purpose, these initiatives have been hindered by lack of administrative support and continuing legal fragility based on the current waiver framework.[135] Therefore, if industry and government leaders want to affect meaningful change to cybersecurity risks, they must start with basic system reforms that reconsider current delivery and payment mechanisms with greater focus. These system reforms will need to continue to consider competing reform goals — quality care, access, and cost control — which remain challenges to the current infrastructure. With careful planning, however, many reforms can also impact and help to address threats to cybersecurity. The reforms must be system-wide and implemented across the health care continuum, maintaining focus on mitigation of cybersecurity risk as a key goal of the legislation. The Report has been a first good step to spur the industry to consider cybersecurity as a significant issue in the health care industry. But, meaningful and effective progress in fighting cyber threats will require leaders to reconsider and reimagine a different system ready to face the risks and rewards of an electronic world.

Note

The author has nothing to declare.

References

1. K. Kristof, "Identity Theft Has Never Been More Rampant," CBS News, February 6, 2018, *available at* <https://www.cbsnews.com/news/identity-theft-hits-record-high/> (last visited November 20, 2019).
2. M. Narendra, Study Reports a 500% Increase in Ransomware Attacks against Businesses, *PrivSec Report*, April 30, 2019, *available at* <https://gdpr.report/news/2019/04/30/study-reports-a-500-increase-in-ransomware-attacks-against-businesses/> (last visited November 20, 2019); *see also* J. Swann, "Ransomware Tops List of Health-Care Data Breach Threats," *Bloomberg Law*, May 7, 2019, *available at* <https://news.bloomberglaw.com/health-law-and-business/ransomware-tops-list-of-health-care-data-breach-threats> (last visited November 20, 2019).
3. K. Sheridan, "Exposed Consumer Data Skyrocketed 126% in 2018," *Dark Reading*, February 4, 2019, *available at* <https://www.darkreading.com/attacks-breaches/exposed-consumer-data-skyrocketed-126--in-2018/d/d-id/1333790> (last visited November 20, 2019).
4. K. Zurkus, "Texas Hospital Discloses Third-Party Breach," *InfoSecurity*, December 13, 2018, *available at* <https://www.infosecurity-magazine.com/news/texas-hospital-discloses-third/> (last visited November 20, 2019).
5. Conner Forrest, "Despite Risks, Only 38% of CEOs Are Highly Engaged in Cybersecurity," *TechRepublic*, October 9, 2018, *available at* <https://www.techrepublic.com/article/despite-risks-only-38-of-ceos-are-highly-engaged-in-cybersecurity/> (last visited November 20, 2019).
6. *See Health Information Technology for Economic and Clinical Health Act*, 42 U.S.C.A. § 300jj-34 (2009).
7. Medical records contain sensitive personal information including name, birthdate, social security number, and medical condition. N. Akpan, "Has Health Care Hacking Become an Epidemic?" PBS Newshour, March 23, 2016, *available at* <http://www.pbs.org/newshour/updates/hashealth-care-hacking-become-an-epidemic/> (noting that health data has fewer protections, but more valuable data). *See also* G. Slabodkin, "Ransomware Emerging as Medical Device Cybersecurity Threat," *Health Data Management*, February 20, 2017.
8. *See* Ponemon Institute, LLC, *2018 Cost of a Data Breach Study: Global Overview* (July 2018): 14. Globally, the health care industry experiences less frequent data breaches than other sectors. *Id.* (noting that the health care industry is tied for 13th out of 17 in terms of the frequency of data breaches over the previous year). *But see* M. Green, "Hospitals Are Hit with 88% of All Ransomware Attacks," *Health IT & CIO Review*, July 27, 2016, *available at* <http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html> (last visited November 20, 2019).
9. Ponemon Institute, LLC, *supra* note 8, at 13.
10. *Id.*, at 18. ("Per capita cost is defined as the total cost of data breach divided by the size of the data breach (i.e., the number of lost or stolen records))." *Id.*
11. *Id.* The "Financial" sector experienced annual costs of $206 per capita. The lowest per capita cost was the "Public" sector, at $75 per capita. *Id.*
12. *Id.*, at 17 (defining "abnormal churn" as "the greater than expected loss of customers since the breach occurred").
13. Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care* Industry, 11-12 (June 2017), *available at* <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf> (last visited November 20, 2019) [hereinafter the "Report"].
14. Cybersecurity Information Sharing Act was passed as part of the *Consolidated Appropriations Act of 2016*, Pub. L. No. 114-113, 129 Stat. 2242 (Dec. 18, 2015).
15. 6 U.S.C. § 1533(b) (2015).
16. *See generally* Report, *supra* note 13. The Task Force has also issued a one-year update regarding its ongoing activities. *See* U.S. Dep't of Health & Hum. Servs., Public Health Emergency, *Year One Activity Update*, *available at* <https://www.phe.gov/Preparedness/planning/CyberTF/Pages/OneYearUpdate.aspx> (last visited November 20, 2019).
17. *Id.*; *see also* D. Raths, "Legislating Cybersecurity: Breaches Grab Lawmakers' Attention," *Government Technology*, October 12, 2016, *available at* <https://www.govtech.com/security/Legislating-Cybersecurity-Breaches-Grab-Lawmakers-Attention.html> (last visited November 20, 2019).
18. *See generally* Report, *supra* note 13.
19. Report, *supra* note 13, at 50-52.
20. *Id.*, at 22-27.
21. *Id.*, at 15-16.
22. N. P. Terry, "Pit Crews with Computers: Can Health Information Technology Fix Fragmented Care?" *Houston Journal of Health Law & Policy* 14 (2014): 129, 148 (examines our fragmented system's effects on IT in healthcare).
23. See Report, *supra* note 13, at 31 (suggesting in Action Item 2.3.8 that "Industry and government should consider issuing a grand challenge, soliciting from stakeholders novel incentive structures that could be leveraged to address cybersecurity challenges specific to securing legacy systems, SDL, strategic

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

and architectural approaches, and holistic data flow and system requirements for EHRs…").

24. S. Bunnell et al., *HHS Releases Cybersecurity Task Force Report*, O'Melveny, June 12, 2017, *available at* <https://www.omm.com/resources/alerts-and-publications/alerts/hhs-releases-cybersecurity-task-force-report/?sc_lang=ko-KR> (last visited November 20, 2019) (criticizing the Report for "largely avoiding recommending prescriptive regulation").
25. As will be discussed in more detail *infra*, interoperability can be seen as both a positive in the fight against cybersecurity risk for its ability to assure sufficient resource allocation across industry players (e.g., large hospital systems to small physician offices) to ensure a consistent prioritization of cybersecurity as a necessary focus, and a negative because of the increased risks posed by having even larger amounts of consolidated data subject to exposure. This Article posits that the benefits of resource allocation will outweigh the risks of data consolidation so long as the technology utilized to achieve interoperability contains appropriate mitigation tools. Thus, interoperability as a potential solution to cybersecurity risk is suggested with the understanding that interoperability *must* contemplate data protection as one of its primary goals.
26. 42 U.S.C. § 300gg; §§ 1320d *et seq.*; 29 U.S.C. §§ 1181-1183.
27. Initially promoted with the enactment of HIPAA, Congress later enacted the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 300jj to jj-51 *et seq.* to further spur use of EHRs. *See* D. Blumenthal and M. Tavenner, "The "Meaningful Use" Regulation for Electronic Health Records," *New England Journal of Medicine* 363 (2010): 501, 501; *see also* D. Charles, et al., *Adoption of Electronic Health Record Systems among U.S. Federal Acute Care Hospitals: 2008-2014*, Off. of the Nat'l Coord. for Health Info. Tech., 23 ONC Data Brief 1 (April 2015), *available at* <https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf> (last visited November 20, 2019).
28. A report issued by the Office of the National Coordinator for Health Information Technology (ONC) tracked use of EHRs over time and noted that by 2008 only 9.4% of hospitals had adopted a basic EHR. *See* Charles, *supra* note 27, at 1.
29. Centers for Disease Control, *National Health Records Survey*: *Table. Percentage of Office-Based Physicians Using Any Electronic Health Record (EHR)/Electronic Medical Record (EMR) System and Physicians That Have a Certified EHR/EMR System, by U.S. State* (2017), *available at* <https://www.cdc.gov/nchs/data/nehrs/2017_NEHRS_Web_Table_EHR_State.pdf> (last visited November 20, 2019). The HITECH Act provided incentive payments (and later imposed penalties) for adoption of "certified" EHR technology (CEHRT). CEHRT is technology that "stores data in a structured format" in accordance with certain established standards for use in the Centers for Medicare and Medicaid Services' (CMS) Promoting Interoperability Programs. *See* Centers for Medicare and Medicaid Services, "Certified EHR Technology," CMS.gov, *available at* <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html> (last visited November 20, 2019).
30. Health IT Dashboard, "Non-Federal Acute Care Hospital Electronic Health Record Adoption," *Off. of the Nat'l Coord. for Health Info. Tech.* (2017), *available at* <https://dashboard.healthit.gov/quickstats/pages/FIG-Hospital-EHR-Adoption.php> (last visited November 20, 2019) (citing source data as the ONC/American Hospital Association (AHA), AHA Annual Survey Information Technology Supplement).
31. *See* S. Yanamadala, et al., "Electronic Health Records and Quality of Care: An Observational Study Modeling Impact on Mortality, Readmissions, and Complications," *Medicine* 95 (2016): 1, 1-2, *available at* <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4902473/pdf/medi-95-e3332.pdf> (last visited November 20, 2019).
32. *See, e.g.,* M. Freudenheim, "The Ups and Downs of Electronic Medical Records," *New York Times*, October 8, 2012; B.G. Arndt, et al., "Tethered to the EHR: Primary Care Physician Workload Assessment Using EHR Event Log Data and Time-Motion Observations," *Annals of Family Medicine* 15 (2017): 419, *available at* <http://www.annfammed.org/content/15/5/419.full.pdf+html> (last visited November 20, 2019).
33. *See* D.J. Solove, "HIPAA Turns 10: Analyzing the Past, Present and Future Impact," *Journal of American Health Information Management Association* 84 (April 2013): 22, *available at* <https://library.ahima.org/doc?oid=106325#.XWgDbuNKiUl> (last visited November 20, 2019).
34. *See* K. Zetter, "Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise," *Wired*, September 17, 2015, *available at* <https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scaryhack-thats-rise/>; *see also* D.R. Farringer, "Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals," *Seattle University Law Review* 40 (2017): 937, 954 (noting that the invention of online currency Bitcoin has made ransomware attacks significantly easier for criminals and more difficult to prevent due to the anonymity of the payment).
35. *See* Report, *supra* note 13, at 9.
36. J. L. Tran, "Navigating the Cybersecurity Act of 2015," *Chapman Law Review* 19 (2016): 483, 483.
37. S. 754-Cybersecurity Information Sharing Act of 2015, Senate Republican Pol'y Committee (Aug. 3, 2015), *available at* <http://www.rpc.senate.gove/legislative-notices/s-754_cybersecurity-inforamtion-sharing-act-of-2015>.
38. Cybersecurity Information Sharing Act (CISA) was passed as part of the Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015); *see also* Tran, *supra* note 36, at 485 (noting the purpose of the act to "provide liability protections for information sharing between corporate entities, between corporate entities and the government, and between different government agencies").
39. 6 U.S.C. § 1533(b). Congress directed the Task Force to (a) analyze approaches of other industries to cybersecurity threats; (b) analyze the challenges and barriers that private entities face in connection with cyber risks; (c) consider challenges related to devices and software that connection to EHRs; (d) provider HHS with educational materials on cybersecurity risks for industry dissemination; (e) establish plan for sharing of information regarding cybersecurity threats; and (f) report to Congress on findings and recommendations. *Id.*
40. The six imperatives are: "1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity. 2. Increase the security and resilience of medical devices and health IT. 3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities. 4. Increase health care industry readiness through improved cybersecurity awareness and education. 5. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure. 6. Improve information sharing of industry threats, weaknesses, and mitigations." *Id.*, at 21.
41. *Id.*, at 1 ("The health care industry in the United States is a mosaic, including very large health systems, single physician practices, public and private payors, research institutions, medical device developers and software companies, and a diverse and widespread patient population.").
42. *Id.*, at 16.
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*, at 17.
47. *Id.*
48. *See* M. Miliard, "State and Regional HIEs: 'Don't Count Us Out Just Yet!'" *Healthcare IT News*, January 28, 2019, *available at* <https://www.healthcareitnews.com/news/state-and-regional-hies-dont-count-us-out-just-yet> (last visited November 20, 2019).
49. See Report, *supra* note 13, at 18.
50. *Id.*

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

51. *Id.*
52. *Id.*, at 23.
53. *Id.*, at 21.
54. *Id.*
55. *Id.*
56. *See* Office of the Nat'l Coord. For Health Info. Tech, *Trusted Exchange Framework and Common Agreement (Draft 2)*, HealthIT.gov, July 7, 2019, *available at* <https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf> [hereinafter the "Trusted Exchange Framework"].
57. *21st Century Cures Act*, Pub. L. No. 114-255, 130 Stat. 1033 (2016).
58. The law has myriad goals, other than that purpose specifically listed above. *See* E. Zacharakis Loumbas, Esq., "21st Century Cures Act: A Myriad of Health Law Remedies," *Health Lawyer* 29, no. 5 (June 2017): 31 (noting that the Cures Act was for the purpose of "funding biomedical research and speed the approval of new drugs and medical devices" along with improvements to behavior health coverage and child and family support services).
59. See Trusted Exchange Framework, *supra* note 56, at 4.
60. T. Sullivan, "Why EHR Data Interoperability is Such a Mess in 3 Charts," *Healthcare IT News*, May 16, 2018, *available at* <https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts> (last visited November 20, 2019).
61. Trusted Exchange Framework, *supra* note 56, at 4. Information blocking is effectively when individuals, clinicians, or payers might block access to certain electronic health information even when there are not restrictions, such as HIPAA or HITECH, that would prevent such information from being shared. *Id.*
62. *Id.*
63. *Id.* The Trusted Exchange Framework is to establish a common set of principles for data exchange and the Common Agreement is to set forth terms by which health HINs will voluntarily be governed. *Id.*, at 9.
64. *Id.*, at 17. While suggested, no common framework has been required or is mandatory, but merely voluntary.
65. *See* S.R. Gering, "Electronic Health Records: How to Avoid Digital Disaster," *Michigan State University Journal of Medicine & Law* 16 (2012): 297, 310 (noting the consequences of the theft of a single laptop for two large federal agencies).
66. *Id.* (recognizing the value of allowing those entities with available resources to dedicate such resources to proper security measures and share those resources across sectors).
67. *Id.* This can be evidenced by its reference to release of drafts of the Trusted Exchange Framework and Common Agreement as an achievement in the one year update. *See* U.S. Dep't of Health and Hum. Servs., *Health Care Industry Cybersecurity Task Force Year One Activity Update*, *available at* <https://www.phe.gov/Preparedness/planning/CyberTF/Pages/OneYearUpdate.aspx> (last visited November 20, 2019) [hereinafter, "One Year Update"]. Since publication of the update, ONC has released a second draft both documents. *See* "Trusted Exchange Framework and Common Agreement," HealthIT.gov, Office of the Nat'l Coordinator for Health Info. Tech., *available at* <https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement> (last visited November 20, 2019).
68. *Id.* The Task Force reported approximately two to three updates for each imperative.
69. The Task Force also noted the release of the Medical Device Safety Action Plan and a plan of action related specifically to the development of a "bill of materials" for each piece of medical technology in order to react to malware attacks in a more targeted way. *See* One Year Update, *supra* note 67. *See also* E. Snell, "Healthcare Cybersecurity Threats Require HHS Bill of Materials," Health IT Security, *available at* <https://healthitsecurity.com/news/healthcare-cybersecurity-threats-require-hhs-bill-of-materials> (last visited November 20, 2019) (noting the importance of understanding which medical devices leverage certain protocols to appropriately quarantine devices following a ransomware attack).
70. *Id.*
71. *See* Freudenheim, *supra* note 32.
72. *See* Report, *supra* note 13, at 22.
73. *Id.* at 14.
74. *See, e.g., id.*, at 22, 37.
75. D. Squires and D. Blumenthal, "Do Small Physician Practices Have a Future?" The Commonwealth Fund, May 26, 2016, *available at* <https://www.commonwealthfund.org/blog/2016/do-small-physician-practices-have-future> (last visited November 20, 2019) ("But an important study…revealed that patients of physicians practicing in solo and small practices have lower rates of preventable readmissions than those in larger practices. Furthermore, many patients and physicians deeply value the personal relationships that smaller settings can cultivate.")
76. See Report, *supra* note 13, at 35.
77. *Id.*, at 35-36.
78. *See id.*, at 11, 14.
79. For example, the Task Force noted that laws like the Physician Self-Referral Law and the Anti-kickback Statute inhibit sharing of resources and information among providers. *Id.* at 27. Competition is another factor that hinders collaboration, but coordination and sharing of resources across sectors could ease some of these business realities.
80. See, T. Hush, "ACO Success: Reaching the Tipping Point," *Becker's Hospital Review*, May 10, 2018, *available at* <https://www.beckershospitalreview.com/accountable-care-organizations/aco-success-reaching-the-tipping-point.html> (last visited November 20, 2019) (noting metrics and care coordination are cultural shifts that have hindered widespread adoption).
81. 42 U.S.C. § 18001 *et seq.* (2010).
82. 42 U.S.C. § 1395nn (2018).
83. 42 U.S.C. § 1320a-7b(b) (2018).
84. 31 U.S.C. § 3729 *et seq.* (2018).
85. See Report, *supra* note 13, at 27.
86. *Id.*
87. 84 *Fed. Reg.* 55766 (Oct. 17, 2019).
88. *Id.*
89. 84 *Fed. Reg.* at 55824-55825.
90. See Report, *supra* note 13, at 27; *see also* 42 C.F.R. § 411.355-357; 42 C.F.R. § 1001.952. Rather than utilize safe harbors or exceptions, many hospitals have chosen to purchase physician practices and/or employ physicians directly to avoid compliance concerns regarding compliance requirements. T.L. Greaney and D. Ross, "Navigating Through the Fog of Vertical Merger Law: A Guide to Counseling Hospital-Physician Consolidation under the Clayton Act," *Washington Law Review* 91 (2016): 199, 200.
91. *See* NCSL Briefs for State Legislators, *Combating Health Care Fraud and Abuse, Health Cost Containment and Efficiencies* (September 2010): 3, Table 2, *available at* <http://www.ncsl.org/portals/1/documents/health/Fraud-2010.pdf> (last visited November 20, 2019). CMS is aware of this issue and has included in its current proposed rules to the Stark Law information blocking as one of the restrictions that would be placed on those who donate EHR software or hardware or, potentially under the proposed regulations, cybersecurity software. *See* 84 *Fed. Reg.* at 55824.
92. Report, *supra* note 13, at 27.
93. *Id.*
94. 42 U.S.C. § 1899 (as added by Section 3022 of the ACA) (establishing the Medicare Shared Savings Program).
95. *See* 42 C.F.R. § 425 *et seq.* Established in 2012 under the ACA, the Medicare Shared Savings Program has been amended in various ways since enactment. *See* 83 *Fed. Reg.* 67816, 67819 (Dec. 31, 2018). There are currently about 1,000 ACOs in operation, with varying success rates. *See* W.K. Bleser, et al., "Following Medicare's ACO Program Overhaul, Most

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

ACOs Stay — But Physician-Led ACOs Leave at a Higher Rate," *Health Affairs*, March 15, 2019; M. Castellucci, "Fewer ACOs Joining Medicare Shared Savings Program," *Modern Healthcare* (July 17, 2019), *available at* <https://www.modernhealthcare.com/accountable-care/fewer-acos-joining-medicare-shared-savings-program?utm_source=modernhealthcare-am-thursday&utm_medium=email&utm_campaign=20190718&utm_content=article2-headline> (last visited November 20, 2019).

96. See Report, *supra* note 13, at 10-11. (noting challenges posed by connecting devices that were not originally established to connect).
97. *See, e.g.,* Dep't of Health and Hum. Servs., *HHS Extends Comment Period for Proposed Rules to Improve the Interoperability of Electronic Health Information*, Press Release, April 19, 2019 (extending the deadline for comment to June 3, 2019). Unlike insurance reforms and payment reforms contained within the ACA, laws promoting EHR interoperability appear to have been less political and easier to move forward in Congress. *See* D. Pittman, "Bipartisan Worry on Federal Health IT," *Politico*, July 24, 2014; *see also* Senator Angus King, *King, Kaine, Isakson Introduce Bipartisam Bill to Modernize Public Health Data Systems*, Press Release, June 12, 2019.
98. *See* Office of the Nat'l Coordinator for Health Info. Tech., *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, Final Version 1.0, at vi-vii, *available at* <https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf> (last visited November 20, 2019) (providing a timeline of all interoperability efforts).
99. *See* C.A. Tschider, "Enhancing Cybersecurity for the Digital Health Marketplace," *Annals of Health Law* 26 (2017): 1, 4-5. The FDA describes "digital health" to include "mobile health, health information technology, wearable devices, telehealth, telemedicine, and personalized medicine." *Id.* While the NIST Framework does provide some guidance, it is voluntary and there is not widespread adoption across the industry of NIST standards.
100. *See* Report, *supra* note 13, at 17. *See also* S.J. Shackelford, et al., "Securing the Internet of Healthcare," *Minnesota Journal of Law, Science & Technology* 19 (2017): 405, 409-410.
101. *See* Report, *supra* note 13, at 22.
102. U.S. Dep't of Health and Human Servs., Food and Drug Admin., *Postmarket Management of Cybersecurity in Medical Devices*: *Guidance for Industry and Food and Drug Administration Staff,* at 6 (December 28, 2016) [hereinafter, "FDA Postmarket Guidance"].
103. *See* Report, *supra* note 13, at 10.
104. *See Id.*, at 11.
105. *See supra* notes 96-98.
106. Food and Drug Administration, "About FDA," *available at* <https://www.fda.gov/about-fda/what-we-do> (last visited July 26, 2019); *see* Tschider, *supra* note 99, at 16-17.
107. *See* K. Booth Wellington, "Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions," *Santa Clara High Technology Law Journal* 30 (2014): 139, 158.
108. 71 *Fed. Reg.* 8389, 8391 (Feb. 16, 2006).
109. *Id.* The HITECH amends HIPAA and thus penalties are imposed by the Office for Civil Rights.
110. *See* 42 U.S.C. § 1395nn (2018); 42 U.S.C. § 1395nn (2018); 15 U.S.C. § 1 (2018) (The Sherman Act); 15 U.S.C. § 18 (2018) (The Clayton Act).
111. *See* Dep't of Health and Hum. Servs., Office for Civil Rights, *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, *available at* <https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf> (last visited November 20, 2019); FDA Postmarket Guidance, *supra* note 102, at 6.
112. *See* Report, *supra* note 13, at 21.
113. *Id.*
114. This article is not suggesting that the authors of the Report intend for the Report to be a manual for industry participants to stop cyberattacks. On the contrary, the Task Force acknowledges in the Report that some of the suggested changes *must* be legislative and/or administrative in nature. This article is suggesting, however, that having identified the necessary issues — some of which are systemic to the health care industry more generally — other steps must be adopted that do not feature cybersecurity as the driving force.
115. While most details about Medicare for All have been very high level, there has been little mention of cybersecurity or interoperability as one of the goals. *See, e.g.,* H.R. 676, "The United States Nat'l Health Care Act," or "Expanded & Improved Medicare For All" (2019).
116. United Kingdom's public health care system, the National Health Service (NHS), experienced the breach referenced herein.
117. M. Field, *WannaCry Cyber Attack Cost the NHS £92m as 19,000 appointments cancelled*, The Telegraph (Oct. 11, 2018).
118. *See id.*; *see also* C. Page, "NHS Admits Windows XP Is Still Running on More Than 2,000 Systems," *The Inquirer*, July 17, 2019.
119. *See* C. Newdick, "Resource Allocation in the National Health Service," *American Journal of Law & Medicine* 23 (1997): 291, 291-295. *See also* D. Maguire, "Interoperability and the NHS: Are They Incompatible?" *The King's Fund*, August 8, 2016, *available at* <https://www.kingsfund.org.uk/blog/2016/08/interoperability-and-nhs> (last visited November 20, 2019).
120. B.R. Furrow et al., *Health Law: Cases, Materials and Problems*, 8th ed. (West Academic Publishing, 2008): at 931-32, 964-65.
121. *See* K. Kane, "How Much Does Quality Cost? Analyzing the Patient Protection and Affordable Care Act's Value-Based Purchasing Provision and How It Could Affect the Delivery of Care by Hospitals," *Duquesne Business Law Journal* 14 (2011): 69, 74.
122. Admittedly, having a comprehensive cybersecurity program will not prevent attacks, but may reduce expense in responding to the attack and shutting an attack down more quickly.
123. *See supra* notes 76-80.
124. 42 U.S.C. § 1395jjj.
125. *See* S. Bires et al., "Clinically Integrated Networks: Guidelines and Common Barriers for Establishment," *Medical Economics*, March 27, 2019, *available at* <https://www.medicaleconomics.com/business/clinically-integrated-networks-guidelines-and-common-barriers-establishment> (last visited November 20, 2019).
126. This should include not just small providers, but also safety net institutions that provide services to indigent populations. Current access issues for indigent populations further reiterates the ultimate argument of this article that system reform is a necessary first step to truly addressing cybersecurity, as providers are unlikely to include these safety net providers in proposed care delivery models due to the challenges of payor mix in making such models financially viable. *See* M. Meidell, "ACOs Face the Demographics Dilemma of Managed Care," *Annals of Health Law Advance Directive* 25 (2015): 14, 20-21.
127. U.S. Dep't of Health and Hum. Servs., "Defining the PCMH," Agency for Healthcare Research and Quality, *available at* <https://pcmh.ahrq.gov/page/defining-pcmh> (last visited November 20, 2019).
128. *See* D.W. Bates, "Physicians and Ambulatory Electronic Health Records," *Health Affairs* 24 (Sept. 1, 2005): 105, *available at* <https://www.healthaffairs.org/doi/full/10.1377/hlthaff.24.5.1180> (last visited November 20, 2019).
129. This is not to say that ACOs are the means by which cybersecurity can be addressed most effectively. Rather, it is to point out that reform efforts exist that could help ease some of the risk because the function of the ACO infrastructure will allow for sharing and collaboration of data without running afoul of existing regulatory and statutory limitations.

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)

130. 42 C.F.R. § 425 *et seq*. While interoperability is not a requirement for ACOs or CINs, studies indicate that ACOs that have a single EHR throughout the ACO prove more effective in meeting quality metrics and thus maximizing the amount of possible shared savings. *See* J. Kim Cohen, "Separate EHRs Pose Care Coordination Challenge for ACOs, OIG Finds," *Modern Healthcare* (May 22, 2019), *available at* <https://www.modernhealthcare.com/operations/separate-ehrs-pose-care-coordination-challenge-acos-oig-finds?utm_source=modern-healthcare-am-wednesday&utm_medium=email&utm_campaign=20190522&utm_content=article2-headline> (last visited November 20, 2019).
131. Ponemon Institute, LLC, *supra* note 8, at 7.
132. *See* Ctrs. for Medicare and Medicaid Servs., "Accountable Care Organizations (ACOs): General Information," *available at* <https://innovation.cms.gov/initiatives/aco/> (last visited November 20, 2019).
133. G.M. Nussbaum, et al., "Securing Connected Devices in Health Care: Taking Proactive Action," *Journal of Health & Life Sciences Law* 12 (2019): 84, 87-93.
134. *See supra* note 92.
135. *See* S. Livingston, *Successful Medicare ACOs Engage Physicians, Patients, Federal Report Finds*, Modern Healthcare (July 24, 2019), *available at* <https://www.modernhealthcare.com/accountable-care/successful-medicare-acos-engage-physicians-patients-federal-report-finds?utm_source=modern-healthcare-am-wednesday&utm_medium=email&utm_campaign=20190724&utm_content=article1-headline> (last visited November 20, 2019).

The Journal of Law, Medicine & Ethics, 47 S4 (2019): 91-102. © 2019 The Author(s)