Emory Corporate Governance and Accountability Review

Volume 4
Issue 0 *Presidential Inauguration Issue*

2017

A Wish-List from the Trenches of Health Information Technology

Sam Snider

A WISH-LIST FROM THE TRENCHES OF HEALTH INFORMATION TECHNOLOGY

Sam Snider[*]

During the 2016 U.S. Presidential campaign, President-elect Donald Trump outlined a seven-point plan for Healthcare Reform[1] that began with a call for the immediate repeal of the Patient Protection and Affordable Care Act[2] (the ACA), enacted in 2010 and more commonly known as "Obamacare." With President-elect Trump's November 29 announcement of Rep. Tom Price, R-Ga., and author of six consecutive versions of a bill proposing full replacement of the ACA, as his nominee for Secretary of the Department of Health and Human Services (HHS)[3], President-elect Trump is continuing to focus on healthcare cost containment and consumerization efforts. However, as the head of HHS, Rep. Price will also need to spend considerable focus on the regulation and oversight of the health information technology (HIT) systems that form the backbone of our modern and evolving healthcare system.

As an orthopedic surgeon, Rep. Price is well versed in HIT matters. While in Congress, he was an advocate of flexibility in the implementation and enforcement of the Centers for Medicare and Medicaid Services (CMS), Meaningful Use Program, and reducing providers' reporting requirements under the Health Information Technology for Economic and Clinical Health

---

[*] Sam Snider is Chief Legal & Compliance Officer at Greenway Health, a leading provider of health information technology to ambulatory healthcare practices whose practice management and electronical health record software and services are used by nearly 100,000 physicians processing over 2.5 billion clinical and financial healthcare transactions each year. The opinions expressed in this Article are solely those of Mr. Snider, and do not reflect the views of Greenway Health or any other individual employed by Greenway Health. The author wishes to thank Mr. David Heller for his assistance with respect to the 21st Century Cures Act.

[1] *Healthcare Reform to Make American Great Again*, DONALDJTRUMP.COM (2016), https://www.donaldjtrump.com/positions/healthcare-reform. Consisting of immediate repeal of the ACA; allowing health insurance sales across state lines; making health insurance premiums tax deductible; allowing health savings plan contributes to be tax free; accumulate over time, and become part of a person's estate not subject to a "death penalty"; requiring price transparency from healthcare providers; funding Medicaid through block grants to states and allowing individual states to administer Medicaid, including preventing fraud, waste and abuse; and, providing freer access to U.S. markets for foreign drug manufacturers.

[2] Patient Protection and Affordable Care Act, 42 U.S.C. § 18001 (2010).

[3] Within HHS, and therefore under Rep. Price purview, are the Office of the National Coordinator for Health Information Technology (the "ONC"), which focuses on technology transformation matters, and the Office for Civil Rights ("OCR"), which focuses on privacy policy and regulatory enforcement.

Act ("HITECH Act") of 2009. As a result, I would expect that HIT matters will be a priority for HHS under Secretary Price, although taking a backseat to his initial focus on amending or repealing the ACA.

This Article provides my personal wish-list of items that I would like to see HHS, and in particular the Office of the National Coordinator for Healthcare IT ("ONC") and the Office for Civil Rights ("OCR"), address during President-elect Trump's term. I believe that these suggestions would significantly enhance the ability of the U.S. healthcare system to provide safe and cost-efficient patient care, while facilitating the exchange of healthcare data throughout the healthcare system My wish-list focuses on four areas: Interoperability, Privacy and Consent, Information Security, and Industry Involvement.

I. INTEROPERABILITY

In September 2015, the ONC released the Federal Health IT Strategic Plan 2015–2020[4], which focused on a vision of "High-quality care, lower costs, healthy population and engaged people"[5] and established four overarching goals for the federal government during the 2015–2020 timeframe: first, advance person-centered and self-managed health; second, transform healthcare delivery and community health; third, foster research, scientific knowledge and innovation; and fourth, enhance the nation's IT infrastructure.[6] My wish-list focuses on the fourth goal of enhancing the nation's IT infrastructure, as I believe it is the foundation upon which the three other goals are built. As is evidenced by the 2015 Plan, and considering that 78% of physicians and 96% of hospitals used certified electronic health record ("EHR") technology, ONC is now heavily focused on three priority areas relating to healthcare interoperability—the seamless and secure flow of health information[7] to any point in the healthcare system in which that information can be beneficially used. As set forth in its 2016 Report to Congress on Health IT Progress (the "2016 Report"), the ONC's three priority areas are:

---

[4] OFFICE OF THE SEC'Y, U.S. DEP'T OF HEALTH AND HUMAN SERV.S & OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., FEDERAL HEALTH IT STRATEGIC PLAN 1 (2015), https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf (the "2015 Plan").

[5] *Id*., at 7.

[6] *Id.* at 6.

[7] OFFICE OF THE SEC'Y, U.S. DEP'T OF HEALTH AND HUMAN SERV.S & OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., 2016 REPORT TO CONGRESS ON HEALTH IT PROGRESS 1, 6 (2016), https://www.healthit.gov/sites/default/files/2016_report_to_congress_on_healthit_progress.pdf.

1. Promoting common standards to facilitate the seamless and secure exchange of data, including through the use of standardized, open application programming interfaces ("APIs")
2. Building the business case for interoperability, particularly through delivery system reform efforts that change the way the CMS pays for care to reward quality over quantity of services
3. Changing the culture around access to information through: combating information blocking; ensuring that individuals know they have a right to access and transmit their health information and that health care providers know they must provide access to the individuals; and reminding health care providers that they are legally allowed to exchange information in the course of treatment or coordinating care[8]

A. Continue Current ONC Interoperability Priorities

The first item on my interoperability wish-list for the incoming Trump administration is that it continues supporting the ONC's high level focus as outlined by the 2015 Plan and the 2016 Report. Regardless of political debates of the deep philosophical and practical differences of opinion around healthcare payment and insurance reform, advances in clinical and administrative software technology along with the rise of incredibly sophisticated data mining tools provide the opportunity for meaningful, perhaps revolutionary, advances in the delivery, efficiency, and efficacy of healthcare; in addition, it can provide the foundation for dramatic improvement in the quality and length of the lives of all Americans. There is very little debate about the attractiveness of a world in which one's complete and comprehensive health record is available at any time and at any point of care, or one in which the world's smartest minds have vast quantities of current and complete de-identified data to mine to identify causalities, correlations, and cures, for intractable diseases like cancer and Alzheimer's. These end states simply cannot be accomplished without true data, liquidity, and interoperability within the U.S. healthcare system, and given the number of players within that system—300+ million patients, several hundred thousand doctors, tens of thousands of individual healthcare practices, thousands of HIT vendors, private health insurance companies, federal payers, employers, state governments, etc.—federal leadership is absolutely necessary, though not sufficient, to achieve true interoperability, and the ONC is generally on the

[8] *Id.*

right track. At the ground level, however, there are an extremely high number of practice problems that must be solved. The two biggest, in my view, are the need to identify and assign health data, regardless of its provenance (e.g. from a primary care physician, acute care provider, wearable, or home health technology, etc.) to the appropriate patient when a comprehensive record for that patient needs to be compiled, and the development of a single and robust set of technical interoperability standards that allow HIT vendors to develop interface technology once, rather than developing slightly different interfaces or connection types to every HIT platform or tool. The next two interoperability wish-list items address these concerns.

B. National Patient Identifier

The next item on my wish-list is the development of a national patient identifier. An individual's health data is generated from a huge number of sources—one's primary care physician, every specialist one sees, supportive specialists such as radiologists, or acute care providers such as hospitals, afterhours practices, and the like, and increasingly from wearables and home-based devices ranging from consumer devices like FitBits and Apple Watches to glucose monitors, smart scales, and other sources of clinically relevant data. To transition to a person-centered versus provider-centered healthcare system, and to facilitate overall health rather than the treatment of chronic or acute conditions, all of this data, from all of these systems must either "live" in a single record, or be available at any time at any point of care. There are a wide range of strategies currently employed to "match" health data to patients, ranging from patient matching used by individual EHR vendors to match patients within their databases, to efforts such as those of the Sequoia Project working to develop frameworks for "Cross-Organizational Patient Identity Matching"[9], to the College of Healthcare Information Management Executives' National Patient ID Challenge, a "$1 million crowdsourcing competition aimed at incentivizing new, early-stage, and experienced innovators to accelerate the creation and adoption of a solution for ensuring 100% accuracy in identifying patients in the U.S."[10] However, as the description of the CHIME National Patient ID Challenge suggests, even the

[9] *See A Framework for Cross-Organizational Patient Identity Matching Available Now for Public Comment*, THE SEQUOIA PROJECT (2016), http://sequoiaproject.org/framework-for-cross-organizational-patient-identity-matching/.

[10] *CHIME Launches $1M Initiative to Solve Patient Mismatching*, HITCONSULTANT.NET (Jan. 19, 2016), http://hitconsultant.net/2016/01/19/31405/.

most sophisticated organizations today are at best capable of matching data to patients 95% of the time, with more common success rates of less than 50%.

Failed patient matching is not a trivial matter. According to a recent article citing a 2014 ONC study, every instance in which an electronic patient match fails, it costs the Mayo Clinic $1,400, and causes Intermountain Health, a large and extremely sophisticated health system, to spend $4–$5 million annually on technologies and processes to reach the 95% rate noted above.[11] In addition to the administrative burden, the patient health implications of a patient record mismatch are obvious.

A national patient identifier would be a significant step in eliminating both the health and financial impact of poor patient matching. Indeed, a national patient identifier was a component of the first draft of the enabling regulations from the original HIPAA statute in 1996, but was blocked in 1998 due to concerns around privacy, security, and the potential for a "big brother-like, government-controlled database." Legislation prohibiting expenditures on the development of a national patient identifier followed soon after.[12] These concerns are certainly real. As 2015 and 2016 have shown, the healthcare industry as a whole is extremely vulnerable to cyberattacks, and there are important federalism and privacy concerns about the creation of a centralized national patient identifier system. However, the privacy and security concerns already exist, and in many ways are worse in the current system. For example, all patient matching algorithms that I know of rely on a combination of data including name, sex, date of birth, and social security number to match patients. The healthcare payments infrastructure requires the transmission of a substantial amount of personally identifiable information and protected health information, not only for payment, but for adjudication of healthcare claims. Both systems result in a proliferation of PII and PHI into a large number of institutional and individual hands, which could be reduced or eliminated through the use of a national patient identifier.

In short, neither I, nor do most people in the HIT industry (including the ONC), believe that true interoperability is attainable without a national patient identifier. The privacy and security concerns around national patient identifiers already exist and are exacerbated by the current system. Efforts to work around

---

[11] *Can a National Patient Identifier Solve Interoperability Challenges?*, HITCONSULTANT.NET (Feb. 8, 2016), http://hitconsultant.net/2016/02/08/31764/.

[12] *See e.g. A Framework for Cross-Organizational Patient Identity Matching Available Now for Public*, *supra* note ix; *CHIME Launches $1M Initiative to Solve Patient Mismatching*, *supra* note x.

the lack of a national patient identifier are inefficient, will never reach 100% accuracy, and generate a tremendous cost burden on the healthcare system that is ultimately borne by patients and taxpayers. There is significant support for a national patient identifier within both the HIT community and federal regulatory bodies. However, the principle objection to the creation of a national patient identifier—government expansion and intrusion into individual privacy—remains. One of the major drivers of President-elect Trump's victory in the 2016 Presidential campaign was his status as a political outsider and willingness to overturn conventional political processes. I would like to see the Trump administration recognize that the benefits of a national patient identifier outweigh all legitimate concerns, and make this a priority of his healthcare policy.

C. Federally-Mandated Interoperability Standards

My last interoperability-related wish-list item is the development of consistent and federally-mandated interoperability standards. As with the national patient identifier, the development of a consistent set of interoperability standards is not a new idea. Indeed, in the ONC's 2014 policy paper "Connecting Health and Care for the Nation: A Ten Year Vision to Achieve Interoperable Health IT Infrastucture," the ONC identified "Core Technical Standards and Functions" as the first building block of true interoperability.[13] In April 2015, Congress declared it, ". . . a national objective to achieve widespread exchange of health information through interoperable certified EHR technology nationwide by December 31, 2018,"[14] and the ONC issued the Final Version of the Shared Nationwide Interoperability Roadmap (the "Interoperability Roadmap").[15] The Interoperability Roadmap is an ambitious document that outlines a wide range of policy and technical components necessary for true interoperability.

For the most part, however, the Interoperability Roadmap leaves the actual development of these standards to the HIT industry, including networks such as the Carequality initiative, the Commonwell Health Alliance, and to

---

[13] OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., CONNECTING HEALTH AND CARE FOR THE NATION: A 10 YEAR VISION TO ACHIEVE AN INTEROPERABLE HEALTH IT INFRASTRUCTURE 1, 9 (2014), https://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf.

[14] Medicare Access and CHIP Reauthorization Act of 2015, Pub. L. No. 114-10 § 106.

[15] *See* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., CONNECTING HEALTH AND CARE FOR THE NATION: A SHARED NATIONWIDE INTEROPERABILITY ROADMAP i, vi–viii (Final Version 1.0, Apr. 2015), https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf.

standards development organizations ("SDOs") such as Health Level 7 ("HL7") and the National Council for Prescription Drug Plans ("NCPDP"). The ONC has even sought and received pledges from a critical mass of industry players, including the 5 largest health systems and companies which provide 90% of EHRs used by hospitals in America, to commit to facilitating consumer access to their electronic health records, help providers share data and not block electronic health information sharing, and implement federally recognized interoperability standards.[16]

Congress has recently taken another step in the right direction. The new administration must implement the 21st Century Cures Act's interoperability provisions, which were signed into law on December 12, 2016, with overwhelming bipartisan support. Notably, it directs the ONC to convene public and private partnerships to develop a trusted exchange framework and common agreement on health information exchange networks within six months of law's enactment,[17] and subjects both healthcare providers and HIT vendors to civil penalties for information blocking, which is broadly defined under the law.

However, like the Interoperability Roadmap, the law relies on the private sector to guide the implementation of the law and a trusted exchange framework. It directs the Secretary of HHS to give deference to standards published by Standards Development Organizations, like HL7. It leans heavily on the input from the HIT Advisory Committee, whose membership will reflect providers, consumers, health IT developers, and more. Further, health information exchange networks are also not required to adopt the standard. Rather, 21st Century Cures relies on a series of carrots to promote the adoption of its trusted exchange framework, such as allowing federal agencies to make it a requirement in contracts.

The challenge with relying largely on the private sector to establish and implement consistent standards is that the sheer volume of players within the HIT space makes the establishment of a single set of standards nearly

---

[16] *Interoperability Pledge*, HEALTHIT.GOV, https://www.healthit.gov/commitment. Please note that my company, Greenway Health, is a member of several of the networks mentioned in this paragraph, and has made the Interoperability Pledge. Interoperability Pledge from Greenway Health to Office of the Nat'l Coordinator for Health Info. Tech., (Feb. 11, 2016), https://www.healthit.gov/sites/default/files/Greenway-Interoperability-Commitments-Pledge-v5-Signed.pdf.

[17] The common agreement may include: 1) a common method for authenticating participants, 2) a common set of rules for trusted exchange, 3) organizational and operational policies to facilitate information exchange, and 4) adjudication processes for non-compliance.

impossible. No single standard will apply to all data use cases, while at the same time is significant overlap in the data that the various standards seek to support. Although the standards create a common interface mechanism, discrete interfaces must be built between each application within an ecosystem, typically on a database-to-database basis rather than flowing through an interoperability hub, and those interfaces must typically be tweaked for different versions of the software on each end of the interface. Maintaining a single consistent interoperability "engine," even between two large technology vendors, that supports all providers on any version of each vendors' products, becomes a significant technical undertaking that limits HIT vendors' ability to build interfaces for new providers and products, and creates more friction and costs within the healthcare system. Because they typically house the "source" database for much health data, the ONC is encouraging EHR vendors to build and publish open application programming interfaces which would allow anyone to build products that extract data from an EHR database, but this solution is not perfect as it requires non-EHR vendors to write to each EHR vendor's API, and opens the door for significant security and authentication challenges.

Both the federal government and HIT vendors have historically been leery of the ONC mandating or developing interoperability standards for a number of valid reasons. In my view, two of the primary and most compelling reasons have been: (a) because the ONC is not a technology developer itself, it is not well positioned to mandate any particular technical specification and its efforts to do so would likely disrupt existing standards development and data exchange, and (b) establishing a technology standard would handcuff or disrupt interoperability innovation. Both of these concerns remain true. However, with promising new standards such as HL7's FHIR and more robust API-based data exchange, I believe that it is important that the federal government exercise leadership by working with the HIT industry to identify and mandate certain base level standards for healthcare interoperability that every player in the industry can develop toward for certain use cases, thus significantly reducing redundant development costs and freeing innovative HIT vendors to deploy development resources toward platform and system innovation and experimentation with, and development of, interoperability technology that will allow deeper and more robust data exchange and become new baseline standards in the future. ONC has certainly taken steps in this

direction through issuing annual Interoperability Standards Advisories,[18] but for core interoperability functions, I believe that advisories are insufficient, and requirements are more appropriate.

II. PRIVACY, CONSENT AND BREACH NOTIFICATION

The ubiquity of data and uses to which it can be put can raise dramatic privacy concerns, from the somewhat creepy, but relatively innocuous and entirely legal "Target knew my daughter was pregnant before I did" scenario,[19] to far more tragic scenarios such as suicides resulting from the unwanted publishing of private videos on public websites of social media.[20] While consumers are generally incentivized to allow companies to use their shopping data through the use of loyalty cards, discounts, and improved customer experiences, health data presents more challenging privacy issues because a patient is in a much different position when consenting to the use of their data at the point of care, and the data itself is far more sensitive. One common fear is that genetic information indicating a predilection toward certain diseases might be used to deny coverage to a healthy person based on a possible future disease state or be used to deny a job applicant. A funnier example that seems to get the point across more effectively when I conduct HIPAA training is that one doesn't want to learn that their sweet Granny caught a social disease at Woodstock because their friends read about it in the local paper through no fault of Granny's.

Generally, the access to, use of, and disclosure of healthcare data in the U.S. is governed by a principle of informed consent, in which a provider, and in turn that provider's business associates, may use data in the ways to which a patient has consented after being given a description of those uses—hence the "HIPAA forms" each of us seem to sign every time we have any interaction whatsoever with a healthcare professional. Unfortunately, while the general principle of informed consent is, in my view, a good one, technology and use cases have dramatically surpassed the current approach to privacy throughout the healthcare ecosystem.

---

[18] *E.g. Interoperability Standards Advisory*, HEALTHIT.GOV (DEC. 20, 2016), https://www.healthit.gov/standards-advisory.

[19] *See e.g.* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16 2012, at MM30, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&hp=&pagewanted=all.

[20] *See e.g.* Laura Donovan, *Revenge Porn Victim Tiziana Cantone Committed Suicide*, ATTN.COM (Sep. 14, 2016), http://www.attn.com/stories/11379/victim-revenge-porn-commits-suicide-after-video-goes-viral.

The next items on my wish-list all relate to fixing what seems to be at best an outdated, and at worst, a broken system that generates substantial inefficiencies in the healthcare system. First, and most importantly from the perspective of the HIT industry, the U.S. healthcare infrastructure needs to be able to rely on a single consistent set of data consent laws, ideally via federal preemption of the patchwork of federal and state laws and regulations governing healthcare data protection. The ONC, for instance, dedicates an entire section of its website to patient consent for electronic health information exchange, including federal laws governing health information generally (i.e. the HIPAA Privacy Rule), particularly sensitive information (behavioral health information, HIV/AIDs status, student health records and genetic information), together with five studies examining various state laws governing the mechanics of disclosure of certain types of information, as well as varying ages at which a patient *can* consent, at which a patient *must* consent, and at which a minor's health information cannot be transmitted to their parents without the minor's consent.[21]

I certainly recognize the important federalism principles the underlie federal preemption of state laws—particularly when there are radically different perspectives on what constitutes "specially" sensitive data and appropriate ages of consent. However, this bizarre patchwork of consent laws creates dramatic friction in the healthcare ecosystem. Providers are expected to be able to manage a set of laws so complex that the federal government requires entire working groups simply to tabulate them, which requires both personnel and IT resources. HIT vendors can provide some relief if data is adequately segmented, but developing a user-friendly workflow to manage the hundreds of thousands of permutations of regulations requires finite development resources which could be better deployed to developing innovative technology solutions to the problems practices face. Technical breaches, even by the most diligent providers and HIT vendors, can result in significant state and federal fines, as well as private rights of action in some instances. In short, the current patchwork of laws directly limits providers' ability to make patients healthier, increases the overall cost of healthcare in the United States, and stifles exactly the kind of technological innovation that the 2015 Plan hopes to deliver. Federal preemption would be an extraordinarily

[21] *See e.g.* PRIVACY AND SECURITY SOLUTIONS FOR INTEROPERABLE HEALTH INFORMATION EXCHANGE: REPORT ON STATE LAW REQUIREMENTS FOR PATIENT PERMISSION TO DISCLOSE HEALTH INFORMATION, HEALTHIT.GOV (Aug. 2009), https://www.healthit.gov/sites/default/files/disclosure-report-1.pdf.

difficult political challenge, but I would very much like to see the incoming administration try.

The second privacy-related wish-list item is more prosaic: I would like to see the Trump administration continue to support the ONC's efforts to develop "preferred" standards for data formatting that allows sufficient granularity for any recipient of discloser of data to block access to sensitive information. The ONC has taken great strides in this direction already through its Data Segmentation for Privacy and Data Provenance initiatives, which will allow sensitive data to be tagged and treated differently by anyone who receives it. However, simply advocating certain standards are not enough—these standards should be part of the core standards that I argue in Section 1(c) should be federally mandated, and a patient's original consent, given at the point of care at which the data was originated, should follow those data elements wherever they go throughout the ecosystem. Managing diverse data elements is a significant challenge as clinical information exchange networks form. Networks often limit data exchange use cases to the bare minimum usages by the recipient (in one case I am aware of, even limiting data provided through a network to use only for "treatment" purposes, despite HIPAA's allowance that data may be used for "treatment, payment or healthcare operations" purposes—theoretically limiting a provider's ability even to create an insurance claim involving that data). A basic federally mandated data segmentation standard, that covers all protected health information or information subject to higher standards under state or federal law, would allow a technical solution to a problem currently managed via contracting, which creates yet further additional friction and cost for the U.S. healthcare system.

The final wish-list item in this section continues the theme of federal preemption. I would very much like the Trump administration to consolidate state data breach notification laws—particularly those with respect to which there is a federal counterpart—into a single homogenized notification law. In addition to the HIPAA Breach Notification Rule, 47 states, Washington D.C., Guam, Puerto Rico and the Virgin Islands have all adopted breach notification laws. These laws often cover different types of information, have different notification periods, and require different content within the breach notice itself. Although it may appear to be "just paperwork," the patchwork of breach notification rules actually hampers the resolution and remediation of a data breach. This is because resources must be dedicated to identifying the state laws that might apply, crafting applicable communications under that law, and circulating them in the timeframe required. Some states have very fast

notification time periods, which means that the notice a recipient receives may not contain all of the relevant data that is developed during the sixty-day investigation period provided for under the HIPAA statute. When a breach occurs—particularly a large scale breach impacting hundreds or thousands of providers, and potentially hundreds of thousands of patients, all hands need to be focused on solving the problem itself, securing customer data, and making sure patients receive the information and protection that they need as a result of the breach. Peeling off resources to check the laws of every state other than Alabama, New Mexico, and South Dakota does not seem to be the highest and best use of resources that could otherwise be dedicated to solving the problem and communicating with impacted patients during a crisis event.

III. CYBERSECURITY

2015 and 2016 saw a tremendous rise in healthcare cybersecurity incidents, ranging from state-sponsored attacks, sophisticated attacks by criminal organizations, individual attacks on widespread HIT systems such as those perpetrated by the (magnificently named) hacker The Dark Overlord, all the way down to simple ransomware attacks against individual practices.[22] The biggest drivers of criminals' current focus on healthcare are the same as all criminal activity—means, motive, and opportunity. Hacking tools are ubiquitous, and include both applications specifically designed for criminal purposes and commonly available, sometimes free, legitimate tools that can be turned to malicious purposes. Healthcare data is among the most valuable types of data on dark web marketplaces, commanding prices of up to $100 per health record in 2015, ranging from $20–$50 per record in 2016 even after the marketplace was saturated with health records due to the massive breaches in 2015 and 2016[23], and since systems typically hold data on thousands of patients, attacking the healthcare community can be extremely lucrative. The nation's healthcare system generally has a long way to go to catch up to the financial services and other very secure sectors due to a combination of often aging technology, an emphasis on data liquidity and interoperability, and limited resources among many healthcare institutions. As a result, significant investment in cybersecurity is necessary throughout the sector, and the majority of HIT businesses now take cybersecurity extremely seriously.

---

[22] *See Major Healthcare Data Breaches: Mid Year Summary*, HIPPA J. (Jul. 11, 2016), http://www.hipaajournal.com/major-2016-healthcare-data-breaches-mid-year-summary-3499/.

[23] Chris Bing, *Abundance of stolen healthcare records on dark web is causing a price collapse*, CYBERSCOOP.COM (Oct. 24, 2016), https://www.cyberscoop.com/dark-web-health-records-price-dropping/.

However, when a breach occurs, covered entities and business associates often find themselves in a dual role in which some law enforcement views them as the victim of a crime, and regulatory agencies view them as at least complicit in the harm ultimately felt by a patient whose data is stolen by "allowing" the attack to occur. While I do not believe that any governmental agency is well positioned to mandate specific security tools or solutions given the rapidly evolving environment and wide variation in size, scale, and assets within the HIT community, I do believe that there are some fundamental things that regulatory agencies can do to help minimize cybersecurity risks.

The first item on my cybersecurity wish-list is for the Trump administration to lead an attitude shift within the Federal Trade Commission, HHS' Office of Civil Rights, and other cybersecurity regulatory bodies in which hacked organizations are assumed to be victims of crimes, rather than the simple fact of a data breach being treated as evidence of wrongdoing by the victimized business. I recognize that there are statutory penalties associated with data breaches, that there is the potential for real harm occurring to patients if a breach occurs, and that covered entities and business associates do and should have a duty to protect data that is in their possession. However, regulators should not view an organization that is complying with the letter of the HIPAA statute and taking reasonable measures to protect the integrity and security of data in its possession as an adversary in the aftermath of a data breach. Doing so only harms the overall security posture of the nation's HIT infrastructure because it makes it far more difficult to have open information sharing among companies and law enforcement before and during a breach. While criminal networks have the benefit of crowdsourcing advanced hacking tools, covered entities and business associates are forced into silos, and are reluctant to share substantial information even within those silos.

The second item on my cybersecurity wish-list is similar to the first. The Trump administration should require all regulatory bodies, including the OCR and Federal Trade Commission, to adopt an incentive structure for companies that comply with law enforcement investigations of a security incident. The first governmental agencies involved with a major data breach or cyberattack are typically members of law enforcement—either local law enforcement or the FBI's cybercrimes unit. These investigators are charged with identifying and ultimately prosecuting the criminals who conducted the attack itself, and are incredibly well positioned to disseminate information on new threat types, attack vectors and other important intelligence to the cybersecurity professionals who are protecting sensitive information. As noted above,

however, companies are reluctant to aggressively cooperate with law enforcement because they fear that the information shared during an investigation will later be used by regulators to increase fines and penalties or to justify settlements requiring costly long term monitoring programs. No company that has been the victim of a cyberattack should be able to avoid responsibility for their errors or omissions simply by cooperating with law enforcement. However, some form of credit should be given for such cooperation to encourage information sharing that will ultimately improve the overall security of the nations' healthcare infrastructure.

The final security item on my wish-list is the most important. One common thread running through cyberattacks ranging from the largest and most destructive to malware and ransomware attacks on small healthcare practices is that almost all begin with e-mail phishing campaigns, or take advantage of simple and easy to resolve security vulnerabilities. Awareness, both of the threat from unsolicited e-mails and the simple, inexpensive steps that can resolve 85–90% of vulnerabilities, may be the single best way to improve healthcare cybersecurity. Given the promise of widespread interoperability, the entire healthcare system is only as strong as the security of its least security conscious participant. OCR, ONC, and HHS should develop federal programs educating patients and providers on simple things that they can do to enhance their cybersecurity and information assurance programs. This public awareness campaign should be prepared jointly not only with cybersecurity experts, but with actual providers and patients who can help craft clear message understandable by a lay person, and make specific recommendation about the types of actions any computer user can take to ensure they have adopted appropriate security settings in their networked computers and the kinds of inexpensive, off-the-shelf applications that anyone can install and use to protect their network, among other things. I am firmly convinced that one of the primary drivers of the country's poor cybersecurity posture is a fundamental ignorance and fear of cybersecurity, and a misconception that there are very few things that an individual or small business can do to protect themselves. An aggressive awareness campaign, combined with healthcare companies' HIPAA-mandated privacy and security training, could go a long way to alleviating by far the biggest security vulnerability in any network—its users.

IV. INDUSTRY INVOLVEMENT

The last HIT-related area on which I would like to see the Trump administration focus is to aggressively recruit into HHS people with experience within the HIT industry—particularly into the ONC and OCR. Both organizations are, in my opinion, focusing on the right areas. However, the ways in which many regulations go into effect and the timing of new requirements for HIT applications in some ways do as much harm as good. Modern healthcare information technology is incredibly complicated, and many existing applications have roots going back 15, 20, and even 30 years. HIT vendors have a wide range of developmental priorities—ensuring current products remain up-to-date with new regulatory requirements, remediating any security vulnerabilities that arise as a result of new attack vectors, ensuring connectivity and interoperability between all of the players in the healthcare ecosystem, and delivering innovations and feature sets that make products more efficient and useful to providers and less disruptive of their workflow. Development resources, however, are finite, and for larger, more complicated applications, product roadmaps require months or years to fulfill a product vision. As a result, regulations that either directly or indirectly require product changes don't just require short-term work, they can disrupt the long term evolution of applications, and because regulatory and security requirements are "must build", innovation and provider-friendly features suffer.

Similarly, ONC's focus on interoperability, and the development of "recommended" standards, is laudable. However, even if developed with technical experts from industry, these initiatives often break down for non-technical reasons due to conflicting needs and incentives among industry participants, both in terms of their function within the system—e.g. providers, HIT vendors, payers, lab companies, etc.—and among players within each of those functions. Contracting and completely unrelated business realities for each player further exacerbate the challenges of translating regulatory action into concrete systemic changes.

The ONC is well aware of this fact, and does make a concerted effort to engage with industry through working groups, meetings with industry organizations and the like. However, at every meeting I attend it is clear that there is a gulf between those creating policy, and those implementing policy. I believe that it would be extremely beneficial to include industry veterans from each part of the healthcare system not just as advisors or working group members, but actually within the ranks of HHS and the ONC, to bring a wider

range of voices to the policy table and include a perspective on real work consequences and barriers beyond that which is provided through formal feedback that is often heavily stylized and of limited value to regulators.

CONCLUSION

In this Article I have set forth a wide range of "wish-list" items for the incoming Trump administration relating to the country's HIT infrastructure. Some of these items, such as a national patient identifier or federal preemption of state privacy or breach notification laws, would be controversial, and others, such as some of the suggestions around interoperability, would be difficult to implement. None of these ideas are new, and many have been proposed by regulatory, legislative and industry bodies for several years. In each case, these suggestions are driven by the practical benefit to the country's healthcare IT infrastructure. In the 2015 Plan, the ONC established an ambitious goal of transforming the healthcare infrastructure into a system that will allow significant advances in patient care while simultaneously reducing costs. That goal is laudable, but requires marshalling a tremendously varied set of stakeholders into coordinated action. Though by no means comprehensive, these suggestions would, I believe, eliminate some of the roadblocks in the path to achieving that goal.