HHS' HCCIC TAKES A QUANTUM LEAP FORWARD TO SECURE THE HEALTH SECTOR

A Fortunate Solution to the Rampant Risk of Minimalistic, Self-Governing Bureaucracy

BY JAMES SCOTT
Senior Fellow, Institute for Critical Infrastructure Technology

COPYRIGHT © 2017 INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY – ALL RIGHTS RESERVED
HHS’ HCCIC Takes a Quantum Leap Forward to Secure the Health Sector
A Fortunate Solution to the Rampant Risk of Minimalistic, Self-Governing Bureaucracy

August 2017

Authored by: James Scott, Sr. Fellow, ICIT
Support ICIT

Information should be liberated, not commoditized.

This powerful philosophy is the bedrock of the Institute for Critical Infrastructure Technology (ICIT), a nonprofit, nonpartisan 501(c)(3) cybersecurity think tank located in Washington, D.C. Through objective research, publications and educational initiatives, ICIT is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark. Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

http://icitech.org/support-icit/
# Table of Contents

HHS Is Uniquely Suited to Help DHS Improve HPH Sector Cybersecurity ........................................ 3

Why Is the Health Sector Targeted? ........................................................................................................ 5

The Private Sector Cannot Oversee Itself ............................................................................................... 5

Self-Governing Firms Forfeit Long-term Patient Security for Short-term Profits .................................. 5

Web Portal Security Is Not Prioritized ..................................................................................................... 7

Sensitive Devices are Not Secured, Managed, or Encrypted ..................................................................... 7

The Private Sector Relies on Insecure Contractors .................................................................................. 8

Improper Data Handling Results from Minimalist and Negligent Governance ...................................... 9

Insider Threat Remains a Persistent Epidemic ......................................................................................... 9

Under-Regulated Medical Data Mining is an Emerging Threat Vector ............................................... 10

The Foundation of the HCCIC ................................................................................................................ 11

Health Care Industry Cybersecurity Task Force Report .......................................................................... 11

HHS Is Justified in Protecting the Healthcare Sector .............................................................................. 13

The HCCIC Does Not Duplicate the NCCIC; It Augments It .................................................................. 16

The HCCIC Will Improve Small and Medium-Sized Business’ Access to Threat Data ........................... 19

HCCIC will collaborate with ISAOs and ISACs, but they will Not Dominate It ....................................... 20

The NCCIC May Fail Without the HCCIC ............................................................................................... 20

Sources .................................................................................................................................................... 23
HHS Is Uniquely Suited to Help DHS Improve HPH Sector Cybersecurity

American critical infrastructure is being perpetually pummeled by adversarial nation-states, mercenaries, cyber-criminal gangs, and script kiddies. And the most gaping wound among all critical infrastructure silos has always been the health sector. Believe it or not, even with the continuous tidal waves of successful cyberattacks, there is a small yet vocal minority that wants to keep standards low to eliminate regulations to disclose a breach publicly, as well as continue the corrupt practice of self-regulation, limited disclosure, and the introduction of artificial chaos that doesn’t exist. Interestingly enough, the loudest proponents of this self-regulating, cyber-hygienically apathetic, minimal standard ideology have all suffered profound attacks recently that had a financial and reputational impact on their organizations. Instead of becoming more cyber-secure, many have chosen to continue the same dangerous minimalistic practices while simultaneously fighting regulatory efforts that would force them to disclose successful attacks that could have a detrimental effect on customers.

Critics claim that the Department of Health and Human Services’ new cybersecurity intelligence-sharing clearinghouse, the Healthcare Cybersecurity and Communications Integration Center (HCCIC), duplicates the role and function of the Department of Homeland Security’s NCCIC [1]. They argue that the HCCIC shifts the goalposts and benchmarks set by the government that responsible industries are trying to meet [1]. In a sense, the assessment is correct, but the argument only justifies the necessity of HCCIC. However, if the private sector were successful in meeting more than symbolic minimalistic requirements, organizations would not be perpetually compromised. Self-regulating, checkbox-driven security standards mean that compromised organizations achieving the absolute minimum in security still come out as winners in a game that stakes patient data security against the profit margin of the organization, because private organizations continuously shift risk to unwilling and unaware consumers and skirt liability by effectively saying that they “did all they could or was required of them.” This participation trophy winner culture that has been crippling the health community has recently been jolted by the presence of real leadership and powerful collaboration to raise the bar in cybersecurity standards.

HHS is aggressively working with industry to cause meaningful and profound upgrades that finally introduce organizational cybersecurity resiliency across the board. The HHS senior advisor for healthcare-public health sector cybersecurity (SA) is the executive sponsor of the HCCIC and is also the chair of an internal Cyber Security Working Group (CSWG), which is composed of the HHS organizations that have an externally facing cybersecurity role, either as a regulatory function or a service provider. The combination of the SA, the CSWG, and the HCCIC provide a unique structure that allows the agency to integrate the robust capabilities of the FISMA-based security program managed by the CISO with support activities that serve the entire sector. Federal agencies have hard-won experience in the fight to move security away from compliance to dynamic risk management, and HHS is positioned to bring those lessons to
less experienced private sector entities, thereby increasing the resiliency of sensitive systems and improving public trust in the sector.

Section 405 of the Cybersecurity Information Sharing Act requires HHS to work with industry to develop voluntary guidelines for implementing cybersecurity frameworks. This work has been the subject of controversy generated by ISAOs and corporations that have a business model based on proprietary implementations of the NIST Cyber Security Framework. If they were responsible data custodians concerned with protecting patients’ data and mitigating cyberattacks, private organizations would not object to more stringent and systematic security requirements. They would want to be held to higher standards that would elevate their security posture closer to the responsible data custodians that consumers deserve. A quantum leap in health sector security requires health sector corporations to disseminate information to improve the cybersecurity of the sector collectively and collaboratively, and to stop leveraging their positions within ISAOs and ISACs to act as gatekeepers to penalize and subjugate small and medium-sized businesses.

The incessant barrage of healthcare incidents demonstrates that the private entities lobbying against HHS are implying that they are capable of setting meaningful benchmarks or effectively distributing threat data to prevent or mitigate hyper-evolving threats. The evidence shows that this approach has failed to do enough to improve the security posture of the sector away from its status as “lowest-hanging fruit” during adversarial target selection. The dependence on compliance-based security has encouraged the sector to treat the primary risk as audits and fines, rather than address the dynamic nature of the threat it faces. In their incapacity, they have demonstrated the need for a non-partisan, non-political, objective, sector-specific communication hub such as the HCCIC. The HCCIC model moves away from the “fine avoidance” approach to risk management and offers the possibility of leveraging the full capabilities of the public sector, the ISAC, and the NCCIC as a “force multiplier” that can jump-start the anemic security posture of the small and medium-sized organizations that dominate the sector. Instead of heeding the words and propaganda of parties who are financially motivated to oppose improving information sharing and enhancing cybersecurity and cyber-hygiene in the health sector, decision-makers should objectively evaluate whether sufficient benefits and security enrichment have been achieved under the governance of private entities, or if a public organization would act as a more efficient and adept intermediary between DHS’ NCCIC and small, medium-sized, and large health organizations.

The HCCIC does not duplicate the form or function of the NCCIC; it serves as a focal point for small, medium-sized, and large organizations to access, utilize, and implement the information disseminated within the community equally, according to the guidelines set by DHS and governing legislation. Moreover, any minor redundancies in data sharing or security operations serve as secondary checks and communication channels to ensure that organizations have every opportunity to protect electronic health records (EHRs). Data not collected or shared by the NCCIC might be caught and circulated by the HCCIC, or vice-versa.
Why Is the Health Sector Targeted?
Multi-layered attacks against the health sector that combine ransomware, Distributed-Denial-of-Service (DDoS) tools, botnets, sophisticated malware, and cyber-kinetic elements have drastically increased over the past few years. From 2010 to 2013, healthcare organizations reported 949 security breaches that put 29 million patient records at risk. The economic impact of medical identity theft was $41.3 billion in 2012. Over 113 million EHRs have been exfiltrated since 2015. Over 90 percent of hospitals suffered a breach in the last two years. Depending on the level of detail, exfiltrated records sell for $20 to $300 on deep web markets and forums. Sales remain high, and specialized markets are forming [2].

Health systems are the “lowest-hanging fruit” for attackers because of private organizations’ drive to disguise negligent and irresponsible practices as “self-governance,” as well as their propensity to shift risk and liability onto other stakeholders [2]. They claim “adherence to due diligence” or “fear of redundancy” to dissuade increased government regulation and oversight potent enough to ensure that patients are protected from predatory corporations and remote adversaries alike.

Private organizations or collections of for-profit entities cannot be permitted to perpetuate these destructive trends that jeopardize patient safety and security. The high-level focus of DHS on information sharing and increased cybersecurity and cyber-hygiene within the HPH sector is an admirable start to modernizing the security and resiliency of the sector; however, without a dedicated and objective partner at the “ground level,” DHS’s NCCIC will accomplish little in the future. HHS’ offer of the HCCIC has the greatest potential of ensuring the continued success of the NCCIC and the improved security of small, medium-sized, and large health organizations. Below are a few examples of the systemic problems throughout the HPH community that will continue to fester and undermine cybersecurity efforts if the HCCIC is blocked from augmenting the NCCIC by self-serving corporations.

The Private Sector Cannot Oversee Itself

Self-Governing Firms Forfeit Long-term Patient Security for Short-term Profits
In February 2015, Anthem Inc. disclosed an incident that exposed the data of 78.8 million patients. Compromised data contained names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, and income data. Encryption was neither employed nor required to protect data, because without much-needed oversight from independent agencies such as HHS, the private sector defaults to controls that do little but shift liability and risk away from the organization. The data was exfiltrated for weeks beginning around December 2014 by a sophisticated threat actor believed to be the Chinese state-sponsored Deep Panda group that targeted OPM a few months later. The breach was discovered because a system administrator noticed a database query using his identifier credentials, which he did not initiate. At the time, Anthem provided coverage to 37 million US citizens [3]. The impact of the
breach extended to other providers and networks. For instance, the data of 215,000 current and former members of the Blue Cross and Blue Shield of Illinois, which is operated by Health Care Services Corporation (HCSC), may have been exposed as a result of the Anthem breach [4]. Similarly, the EHRs of 51,000 current Highmark health insurance customers in Pennsylvania reportedly were exposed in the Anthem breach [5].

In exchange for immensely jeopardizing the lives and well-being of the public, Anthem paid relatively minuscule fines and settlements, and they offered the actual victims two years of ineffective credit monitoring and identity protection. A modest $15 million of the settlement was set aside to compensate victims for the fiscal harms that they might suffer in the future [3]. The settlement amounts to about $50 per class member [6]. In comparison, medical identity fraud victims spend an average of $13,500 on lawyer fees and false healthcare bills, not considering the monetary value of the approximately 200 hours needed to interface with healthcare organizations and correct exploited records and accounts. Those who fail to correct their records could suffer harm or death if a threat actor uses their medical profile and alters characteristics such as blood type or allergies. [2].

Anthem issued guidance to warn victims of phishing scams and cascading campaigns that would leverage the stolen information in targeted attacks against Anthem patients. It also offered credit freezes for minors’ data. Children’s “fullz” are worth significantly more than adults’ profiles because attackers can exploit the data for years before any exploitation is realized. Most parents do not regularly run credit checks on their children [6].

After disclosure of the incident, Anthem agreed to pay a $115 million class-action lawsuit; however, it specified in a statement that it did not admit any wrongdoing or any responsibility for realized harms [3]. The settlement sum was meager compared to the profit margin of Anthem and the long-term, potentially life-threatening risk to nearly a quarter of the nation. Investors and analysts estimate that the breach barely impacted Anthem’s bottom line or reputation, if at all, because the risk was already shifted to consumers and any lingering liability, such as the identity protections offered to victims, were covered under a cyber-insurance policy [7].

Anthem systems were breached because the organization failed to implement layered defense-grade security solutions. Such robust and comprehensive controls are not mandatory because private organizations, who wish to self-govern the sector, intentionally set ineffective minimalistic checkbox requirements instead of acting in consumers’ best interests. Until an independent agency like HHS oversees the HPH sector on behalf of DHS, private organizations will continue to sacrifice long-term patient security in favor of short-term profits. Due to private sector self-governance and lobbying efforts opposing meaningful governance, Anthem put 78.8 million patients at permanent risk of exploitation in the form of blackmail, financial scams, healthcare fraud, and other harms. In another example, Express Scripts was compromised by extortionists in October 2008. A year later, 700,000 individuals were notified that their information may have been breached during the incident. A few consumers reported being
targeted by attackers using the data. Additionally, Toyota employees, whose pharmacy benefits were managed by Express Scripts, received extortion correspondence [8].

Web Portal Security Is Not Prioritized

Medical data is more valuable to attackers than financial data, and it can easily be exfiltrated from vulnerable web portals. Once an adversary has patient data, they can exploit the individual or file false claims across the sector. Anthem systems remain at potential risk. Its web portal does not secure cookies or use HttpOnly cookies that mitigate the risk of client-side script attacks. It does not have DNSSEC enabled or a 30-day domain period specified. Finally, its server information is not obscured, and the systems may be easily discovered and targeted by script kiddies or more sophisticated adversaries. An UpGuard analysis of the cybersecurity of UnitedHealth Group’s web-security ranked it as the least secure and resilient of those reviewed. It failed eight of 20 measures outright. Its pages did not have SSL or SPF enabled. Server information was not obscured. The credentials of those browsing the site were subject to potential intercept by third parties because the HTTP Strict Transport Security was not properly implemented. Cookies were not secure or HttpOnly, meaning that attackers could copy identity information remotely and use it on another system. DNSSEC was not enabled, so third parties may have been able to forge domain identity records. The server presented unnecessary server version information in the header, and the ASP Net Version header information was exposed [9]. Hackers could use such information when configuring point-and-click tools like Metasploit, when searching for vulnerable systems on services like Shodan, or when tailoring an exploit. Similarly, UpGuard found that Walgreens’ web lacked HTTP Strict Transport Security to prevent man-in-the-middle attacks, that it did not have DMARC enabled to protect against phishing campaigns against the domain, and that DNSSEC was not enabled to prevent threat actors from forging domain identity records. In another example, Kaiser Permanente’s web portal did not have DNSSEC or HTTP Strict Transport Security enabled, and its cookies were neither secure nor HttpOnly [9].

Sensitive Devices are Not Secured, Managed, or Encrypted

Children's Health, formerly known as Children's Medical Center, is the seventh-largest pediatric healthcare provider nationally. In 2009, an employee lost an unencrypted and non-password protected BlackBerry at the Dallas/Fort Worth International Airport containing the electronic health records of 3,800 patients [10] [11] [12]. In 2013, an unencrypted laptop containing 2,462 patients’ data was stolen from the hospital [10] [11] [12]. The hospital had physical safeguards monitoring the laptop storage area, but it provided access to personnel who were not authorized to access electronic health records [12]. While the organization did self-report the incidents, it did not implement technical and policy safeguards strong enough to deter future incidents. According to a federal investigation, Children’s Health had been made aware of risk management gaps in February 2007 after a three-month analysis from Strategic Management Systems. A separate 2008 PwC analysis confirmed the risk and need for more robust security. It advised that encryption be a high priority for the medical center, as lost or stolen devices could
jeopardize patients’ data and health. Nevertheless, Children’s Health declined to change its policies or mandate encryption until April 2013, after the incidents and potentially countless others occurred, according to the Office of Civil Rights investigation. In January, the entity declined its right to request a hearing or challenge the fine [11] [12] [13] [14]. In February 2016, Children’s Health paid a $3.2 million federal penalty resulting from “impermissible disclosure of unsecured” health information [10] [11] [12] [13]. The U.S. Department of Health and Human Services, Office for Civil Rights (OCR) justified the fine, citing Children’s Health’s "non-compliance" over many years with multiple standards of the HIPAA Security Rule [12] [13].

For the hospital, it was likely cheaper to operate insecurely for years and eventually pay a fine than it was to secure systems sooner when it was notified of the risk in 2007. The economics of risk management allow organizations operating in this irresponsible manner to make short-term profits while shirking essential security requirements, transferring risk to consumers until an incident is discovered and their public reputation is challenged. Afterward, they pay minor fines and continue minimally securing sensitive treasure troves of patient data.

In September 2015, Concentra Health Services, a subsidiary of Humana, one of the largest U.S. commercial health insurers, paid $1.7 million in a HIPAA violation settlement related to unencrypted laptop thefts that occurred in 2011 [15] [16]. In October 2015, an encrypted laptop and unencrypted USB device containing the names, dates of birth, and “clinic names” of 2,800 Medicare Advantage Plan subscribers were stolen from an employee’s vehicle [17] [15].

OptumRx is UnitedHealth Group’s free-standing pharmacy care services business, managing more than one billion prescriptions annually. In March 2016, OptumRX notified patients that an unencrypted laptop containing PHI was stolen from a vendor’s vehicle. Records on the system included name, address, health plan name, prescription drug information, and prescribing provider details [18]. In September 2016, OptumHealth New Mexico lost 2,006 EHRs when a vendor mailed an unencrypted flash drive containing the data to an undisclosed recipient. It remains unclear why the drive was posted (using standard USPS) or why the device was not encrypted. Data stored on the drive includes name, medical diagnosis, partial SSN, and other health information [19].

The Private Sector Relies on Insecure Contractors

In January 2017, 19,000 beneficiaries of Highmark Blue Cross Blue Shield of Delaware were notified that their information might have been exfiltrated from compromised contractor systems belonging to Summit Reinsurance Services and BCS Financial Corporation. Those impacted were beneficiaries of 16 employer-paid health plans through Highmark. On August 5, 2016, Summit suffered a ransomware attack, and forensic analysis suggested that their systems may have been compromised by one or more attackers as early as March 12, 2016, or even earlier. Data exposed included Social Security numbers, health insurance details; providers’ names; medical records relating to insurance claims, including medical diagnoses; and some clinical information. Victims were offered a year of credit monitoring and identity restoration services.
These remediation offerings are meager and often meaningless. They do little to protect patients from exploitation. Victims are permanently compromised because medical data does not change. The attacker could wait patiently for a year, and then begin selling the data on deep web markets and forums. The main function of credit monitoring is to deter lawsuits against the negligent organization following an incident. Further, because the contractor sent the letter detailing the incident instead of Highmark, many mistook it for an advertisement or scam. Most consumers have never directly interacted with Summit Reinsurance Services and BCS Financial Corporation. Consequently, they did not see or use the offered remediation services.

Improper Data Handling Results from Minimalist and Negligent Governance

Walgreens is the top pharmacy chain in the United States, and it is prone to regular compromise from insider threat actors as a result of its inability to implement effective governance policies and procedures. Throughout the early 2000s, Walgreens failed to protect consumers’ sensitive healthcare information. In 2006, investigations discovered that Walgreens was disposing of intact paper health records in unsecured dumpsters behind the buildings. Stolen records had enabled a drug addict to locate and rob a relative. While Walgreens did later take actions to improve physical security practices to avoid fines and shake a nine-year investigation, its security of electronic records may follow a similar characteristic pattern of lackadaisical security. In 2010, Walgreens customers were victimized by spear phishing campaigns resulting from stolen email lists from a breached marketing partner. In January 2012, a Walgreens pharmacist was sentenced to 25 months in prison for patient identity theft. In July 2013, a Walgreens pharmacist accessed and exposed her husband’s ex-girlfriend’s information. While the employee was disciplined and the victim filed a lawsuit against Walgreens, it is important to note that the company lacked strong patient privacy policies preventing the incident.

Insider Threat Remains a Persistent Epidemic

UnitedHealth Group is one of the largest healthcare organizations in the nation, and it regularly ranks within the top 20 of the Forbes 500. They and their subsidiaries have proven in the past to exercise lax cybersecurity and have been compromised on multiple occasions. The group’s immense profits may be leveraged to rally against increased regulation and oversight that would mandate responsible cybersecurity and cyber-hygiene controls regarding electronic health records, such as the innovative HHS initiative. According to public Health and Human Services databases, UnitedHealth Group was compromised in 2010 and 2012, affecting 16,291 and 19,100 people in an undisclosed and unauthorized access attack respectively. Also in 2012, an insider threat accessed Medicare members’ data without permission. In its 2013 annual report, UnitedHealth Group cited concerns that its systems were vulnerable to malware, software vulnerabilities, unintentional and malicious insider threats, remote compromise, and other vectors. It proclaimed in a cautionary statement, "We could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm, and other serious negative consequences if we sustain cyberattacks or other privacy or data security incidents that result in
security breaches that disrupt our operations or result in the unintended dissemination of sensitive personal information or proprietary or confidential information” [29] [30].

Similarly, Kaiser Permanente has suffered a plethora of incidents over the past decade [9]. In August 2008, an employee stole 5,200 Kaiser Permanente Falls Church Medical Center personnel records. Six months later, 29,500 northern Kaiser employees were notified that their names, social security numbers, and birthdays had been found in the possession of an apprehended criminal [31]. In late 2009, an electronic portal device was stolen and 15,500 patients were notified. In two incidents in 2013, a flash drive stolen from the Anaheim Medical Center’s nuclear medicine department exposed 49,000 patients, and the records of 647 patients were accessed or disclosed without authorization. The following year, 5,100 patients were notified that malware detected on a server might have accessed, altered, or exfiltrated their healthcare information. The malware may have been present on the system for over two years. Due to “human error related to the configuration of the server,” the anti-virus software had not been updated. Compromised patient data may have included names, date of birth, age, gender and possibly addresses, race/ethnicity, medical record number, lab results associated with research, and research-related questions [32] [33]. On June 10, 2016, two employees stole an unspecified number of ultrasound machines containing protected health information. As of July 11, 2016, 1,136 patients were affected [32]. In November 2016, Kaiser Permanente Health Plan, Inc. of Northern California; Kaiser Permanente Health Plan, Inc. of Southern California; and Kaiser Foundation Health Plan of the Northwest notified 8,020 members that some of their health information may have been viewable to users visiting the site during a two-hour time frame from October 12, 2016 to October 13, 2016 [42].

**Under-Regulated Medical Data Mining is an Emerging Threat Vector**

QuintilesIMS is the dominant medical data and prescription mining company [34]. It buys bulk data from pharmacy chains, doctor's electronic record systems, claims from insurers, and other health information. It anonymizes the data and then sells it or derivative insights to other sector organizations [35]. Data aggregators and brokers pose a significant and under-considered threat to the security and resiliency of critical infrastructure sectors. They have an established history of insider threat incidents and breaches that derive from their aversion to protecting the confidentiality, availability, and integrity of data where it is stored, as it is processed, and when it is in transit. For instance, in 2007, a Ukrainian trader named Oleksandr Dorozhko hacked into IMS Health (which has since merged with QuintilesIMS) and stole information on earnings that he used to make profitable trade options [36]. QuintilesIMS has compiled an estimated half a billion comprehensive dossiers on patients using self-reported and inferred details.

Even though data sets are anonymized, attackers can leverage an abundance of metadata against the sets to re-identify individuals and blackmail or otherwise exploit them. Consequently, adversaries are already launching precision targeted attacks against critical infrastructure owners and operators, using metadata and exposed data sets to tailor spear-phishing lures, watering-hole
sites, drive-by-download landing pages, malicious fake news stories, propaganda narratives, and other nascent vectors against high-value critical infrastructure targets [37]. Despite the risk to individual privacy and public security, medical data brokers continue to sell segmented and categorized patient lists. Data often includes addresses, phone numbers, or e-mail addresses, which can easily be used to identify the data subject. One website aggregating offerings from different data brokers offers categories such as People with Cancer by State, Booming Boomers with Erectile Dysfunction, Bladder Control Product Buyers list, Heart Disease Sufferers Email/Postal/Phone Mailing List, and STD Mater (of “mature singles that may have a sexually transmitted disease”) [38]. Others forgo categorization by condition and instead profile individuals by lifestyle.

Medical organizations have also begun “propensity modeling” data sets by combining dossiers of patients with separate anonymized data broker files. Algorithms are employed to predict what conditions people might have based on a broad data set, then market to individuals directly. Identifiable metadata from user visits to web pages may also be cross-referenced against detailed dossiers or broad patient sets [38]. The highly detailed and precise product analysis is then stored on healthcare data broker systems, which may already be compromised because of a sector-specific reliance on security theater and opposition to the common-sense oversight of a sector-specific agency, like HHS and its HCCIC.

The Foundation of the HCCIC

Health Care Industry Cybersecurity Task Force Report

As part of the Cybersecurity Act of 2015, Congress required an established Health Care Industry Cybersecurity Task Force to review and analyze the trials and tribulations obstructing healthcare organizations in their attempts to ensure patient privacy, safeguard data security, and respond to intentional and unintentional cybersecurity incidents. The findings of the Cybersecurity Task Force led to the foundation of the Healthcare Cybersecurity and Communications Integration Center (HCCIC). Seventeen private sector members and four public sector task force members were assembled at the behest of HHS’ secretary in consultation with the NIST director and the secretary of the Department of Homeland Security. Throughout the lifecycle of the program, industry participants identified a complex range of threats against the healthcare community. Over the course of a year, using information gathered during public meetings, briefings, and consultations with experts on a plethora of healthcare and other critical infrastructure topics, internal task force meetings, and responses to blog posts and information gathered from external stakeholders and subject matter experts across the healthcare industry and other sectors, the task force identified six high-level imperatives under which to organize the recommendations and action items.
The six imperatives outlined by the task force are:

1. Acknowledging the diverse needs of a wide array of stakeholders across the health care industry to define and streamline leadership, governance, and expectations for health care industry cybersecurity, the task force recommends the creation of a "cyber leader" role within HHS to coordinate industry engagement across regulatory and voluntary cybersecurity programs. They identified the need for HHS to promote clear and consistent cybersecurity discussion, oversight, and engagement. The Task Force further recommends the streamlining, harmonization, and propagation of cybersecurity efforts and best practices across the industry. The unique needs and differing capabilities of small and medium-sized organizations were considered in comparison to similar attributes of larger organizations.

2. Medical devices and systems containing electronic health records (EHRs) are notoriously vulnerable to remote adversarial compromise because they traditionally lack any form of security-by-design throughout the developmental lifecycle of the device. As a result, the task force prioritized increasing the security and resiliency of medical devices and health IT. The task force recommends that HHS evaluate opportunities for strengthening public/private relationships and leverage the progress already made by associations and groups that have brought the private sector together around cybersecurity challenges. They recommend a total product lifecycle approach, comprised of a mix of regulation, accreditation, information sharing, and voluntary development and adoption of standards to promote system security from product design and development through the end of life.

3. Prioritize and ensure cybersecurity and cyber-hygiene awareness and technical capabilities in a developed healthcare workforce. They delineate the predominant barriers restricting cyber initiatives in small, rural, and other lesser-resourced organizations. It recommends enhancing cybersecurity leadership in organizations, developing the healthcare cybersecurity workforce, and creating options for organizations to share cybersecurity services and gain efficiencies.

4. Improve healthcare industry readiness by improving cybersecurity training, awareness, and education, mainly by raising awareness among corporate leadership, educating employees on cybersecurity and cyber-hygiene, and empowering patients to make better choices related to the security of their personal health information. The task force recommends that HHS and industry partners promote cybersecurity awareness across health care.

5. Implement solutions that secure R&D efforts and intellectual property (such as clinical trials, device development, drug research, big data applications, and general healthcare business operations) from attacks or exposure. The task force recommends increasing the
industry's understanding of the scope of the problem and the economic and other risks of continuing intellectual property loss.

6. Expand information sharing of indicators of compromise (IoCs), industry threats, risks, and mitigations. Recommendations focus on the sharing of cyber threat information among government and industry partners. The task force recommends general principles to follow in the establishment of cyber-threat information sharing systems in healthcare, with a focus on ensuring that curated and actionable information reaches small and rural organizations.

Executive Order 13800 held department secretaries accountable for agency information security management, governance, and policy. The Cybersecurity Act of 2015 required the HHS Cyber Threat Preparedness Report, which identified the HHS deputy secretary as the official overseeing cybersecurity within the department. The HHS deputy chief information security officer serves as the senior advisor for cybersecurity to the secretary and as the Chair of the HHS Cybersecurity Working Group, the principal forum for coordinating cybersecurity support and response across all HHS operating divisions and staff divisions. It provides support and outreach to the HPH sector by efficiently allocating HHS resources, leveraging critical capabilities, and augmenting public-private communication channels to improve incident preparedness, awareness, detection, response, and remediation efforts. HHS’ focus on communication and the influx of resources it will provide can phase out ineffective minimalistic and checkbox frameworks that amount to security theater. The senior advisor for cybersecurity will align and coordinate internal stakeholders to collaborate with the private sector, the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST), and the U.S. Department of Homeland Security (DHS) to develop voluntary guidelines to support adoption of the NIST Cybersecurity Framework and support HPH sector risk reduction and resiliency [39].

**HHS Is Justified in Protecting the Healthcare Sector**

The healthcare space is considered especially difficult to secure universally against digital adversaries because it consists of entities ranging from single-doctor practices to multi-national insurance firms, and it depends on highly valuable electronic health records (EHRs). The sector needs new leaders who are capable of interfacing with all stakeholders, agencies, and legislators [40]. HHS is already at the forefront of healthcare cybersecurity, and its role as intermediary with the NCCIC through the HCCIC is an optimal and efficient solution to decreasing the vulnerability and exploitability of a siloed sector that has been too long starved for objective sector-specific attention and assistance. HHS bears a plethora of healthcare and public health responsibilities, ranging from the Food and Drug Administration’s role in medical devices to the Centers for Medicare & Medicaid Services’ role in electronic health records to the Center for Disease Control and Prevention’s role in protecting public health. Through the Presidential
Policy Directive 21 (PPD-21), HHS was designated as the Sector Specific Agency (SSA) for the healthcare and public health (HPH) sector because of the complexity and size of its mission and its important and established role in coordinating cybersecurity preparedness with the private sector. As an SSA, HHS coordinates with DHS to facilitate and incentivize cybersecurity and resiliency in public-private collaboration within the HPH sector. HHS responds to sophisticated emerging threats by leveraging unique federal government and private sector expertise and partnerships.

The emergency response role the HHS plays in the sector is often underestimated. In the event of a natural disaster, the secretary of HHS, through the assistant secretary for preparedness and response (ASPR), provides manpower, material, and logistical support to the affected entities. The Office of Inspector General provides law enforcement and investigative capabilities that augment the local and federal law enforcement agencies, and the Secretary’s Operations Center (SOC) coordinates all of these capabilities while providing links to the intelligence community and the NCCIC through the HHS Office of Strategic Security and Intelligence (OSSI). This is a robust emergency response capability that is activated many times each year in response to hurricanes, floods, and other natural disasters.

All of this is part of the agency's Critical Infrastructure Protection Program and operates under the authorities of PPD 41 and the National Cyber Incident Response Program (NCIRP). PPD 41 states, "When a cyber incident affects a private entity, the federal government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant sector-specific agency (SSA) will generally coordinate the federal government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure." The HCCIC has integrated the cybersecurity expertise and analytic capability that this program lacked previously. This is a unique commitment of cybersecurity resources to such a program, both within the federal government and in the emergency response community at large, and is another indication that HHS is “leaning in” to the challenges facing the sector.

A critical partner in that effort is the National Health Information Sharing and Analysis Center (NH-ISAC), which won competitive grants issued by ASPR and the Office of the National Coordinator (ONC) last year. These grants were designed to encourage the ISAC to provide cybersecurity services to its members and non-members alike. NH-ISAC has partnered with HCCIC in that effort, and this alliance has also come under fire as an inappropriate action by the government and duplicative of capabilities that are provided by DHS. The criticism is both shortsighted and inconsistent with federal directives. The NCIRP clearly states the role of the NH-ISAC as an essential partner for the SSA. The relationship of the HCCIC to the NH-ISAC is a model implementation of that statute and should be emulated by SSAs and the emergency response community in general. Cyber events are “kinetic” events with wide-ranging and
potentially life-threatening impact. The public-private partnership is an approach whose time has come and needs to be looked at as an essential part of the government’s relationship to the private sector.

According to Aetna Chief Security Officer Jim Routh, “Public-private partnership is an essential component to improve the resilience of healthcare organizations in the U.S. The NH-ISAC works collaboratively with the HCCIC around the clock to understand the implications for cybersecurity incidents and share information essential to the protection of healthcare information.” Routh contends the new HCCIC will potentially expand cyber threat information sharing in the healthcare industry, rather than be duplicative of efforts at NH-ISAC or HITRUST.

For a decisive proof of concept of how well-suited HHS is for this emerging role, consider that through its Office of the Assistant Secretary for Preparedness and Response (ASPR), HCCIC was integral in the health sector response to the WannaCry ransomware attack that cryptographically crippled dozens of U.K. hospitals as well as organizations across the globe. In the U.S., HCCIC, with collaboration from the NH-ISAC, immediately designed and implemented a health sector-specific strategy that informed health IT professionals how to respond to NCCIC and US-CERT guidance and thereby prevent, mitigate, respond to, and report WannaCry infections. During the attack, the HHS security staff successfully focused on protecting its internal systems and assets while simultaneously assisting private organizations to identify and combat the emerging threat.

The information channels developed by ASPR were fully used with no need to develop new “cybersecurity” channels or duplicate any existing capabilities. The response included conference calls, with up to 3,100 lines open and an estimated 5,000 to 7,000 participants, daily FAQs, and a catalog of available federal resources [40]. The HCCIC helped NH-ISAC identify the five appropriate controls for mitigation that were then shared with all members of the HPH community [37].

To support organizations responding to incidents more effectively, HCCIC will be collaborating with sector partners to make available the data, tools, and strategies to enhance and support HPH sector cybersecurity initiatives in steady-state mode as well as in emergencies. ASPR has already assembled a library of peer-reviewed cybersecurity resources to train healthcare stakeholders to better protect against, mitigate, respond to, and recover from cyber threats to defend patient safety better and ensure operational continuity. The Fiscal Year 2018 budget includes a $21 million increase for the development and expansion of HHS’ cybersecurity threat and information sharing capabilities across the federal and private healthcare space. Further, HHS is establishing and sustaining valued cybersecurity industry partnerships; providing analysis of incidents, threats, and vulnerabilities; maintaining post-incident and risk-informed trending and analysis; sharing healthcare and public health specific lessons learned across the sector; and enabling healthcare and public health partners to make actionable risk-based decisions.
The HCCIC Does Not Duplicate the NCCIC; It Augments It

HHS’ HCCIC aims to support NCCIC in its mission to provide timely, ubiquitous, and accessible cybersecurity and incident response services to the entire healthcare community. It is not a duplicate of the NCCIC in intended operational form or functionality; anyone proselytizing otherwise is propagating a selfish agenda with the intent of maintaining an asymmetrical status quo in the HPH space where healthcare entities are vulnerable; patients are exploited; and the sector is dependent on negligent, avaricious, gatekeeper entities that stifle small and medium-sized business and innovation and jeopardize patient security for the sake of profit. The HCCIC was modeled after the National Cybersecurity Communications Integration Center (NCCIC) with the assistance of the Carnegie Mellon University Software Engineering Institute (CMU-SEI) to be a sector-specific cybersecurity coordination hub between the HPH sector and the NCCIC. The HCCIC will enable US-CERT to interface with isolated, lackadaisical, and under-resourced health sector organizations that would not otherwise engage with national cybersecurity initiatives. Many of the targeted organizations are small and medium-sized businesses that remain underserved because they lack the resources to initiate meaningful dialogue with the NCCIC and their insignificance forgoes continuous attention from DHS. Unlike private sector organizations, HCCIC will have dedicated personnel maintaining direct communication with the NCCIC for near-real-time intelligence sharing and threat response. Further, the NCCIC has a dearth of healthcare-specific context to multi-sector threats and incidents.

A close examination of the authorities that NCCIC and HCCIC operate under demonstrates that HHS is acting appropriately as a strong sector agency in this regard:

The NCIRP provides very clear roles and responsibilities for the different layers that make up the cybersecurity response "stack." It first establishes the primary role of the sector ISAC as a sector-specific entity, particularly in relation to ISAOs and other sub-sector entities, emphasizing, “Most private sector operational information sharing is conducted through ISACs. ISACs are typically a sector-based type of Information Sharing and Analysis Organization (ISAO) and operate through a defined sector-based model, meaning that organizations within a certain sector (i.e. financial services, energy, aviation, etc.) join together to share information about cyber-threats… Unlike ISACs, ISAOs are not necessarily tied to critical infrastructure sectors.”

It goes on to note, “SSAs also play a role in sector coordination, working closely with DHS and serving as a day-to-day federal interface to prioritize and coordinate activities within their respective sectors; carrying out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and providing support or facilitating technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate…”

Reiterating the language of its parent statute (PPD 41), the NCIRP then describes the operational relationship between DHS and the sector-specific agency:
“DHS, working with relevant SSAs, also coordinates the government’s efforts to understand the potential business or operational impact of a cyber incident on critical infrastructure in a given sector and across sectors. The relevant SSA will generally coordinate the federal government’s efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure. SSAs receive support from the DHS NCCIC and the National Infrastructure Coordinating Center to maintain and provide situational awareness on threats, incidents, or events impacting critical infrastructure and to facilitate information sharing. This includes a near-real-time capability to provide SSA reports, coordinated with FEMA ESF reporting provided by the National Response Coordination Center, and the capability to solicit and receive information on incidents from public and private sector critical infrastructure partners. Because SSAs often have authorities, responsibilities, and partnerships with private industry that extend beyond security and resilience issues, SSAs play a lead role in integrating response to the technical aspects of cybersecurity incidents with efforts to mitigate the systemic impacts of such incidents to sectors…”

The ability to link private sector entities and the context they provide to intelligence information during an incident is a fundamental purpose of the multi-layered structure the statute envisions: “When determining incident severity, DHS, through the NCCIC and the SSAs of sectors affected or likely to be affected, may consult with sector leadership and private sector owners and operators through organizations such as the sector ISAC(s), SCC, GCC, the National Council of ISACs, MS-ISAC, and/or the Partnership for Critical Infrastructure Security if the incident affects or is likely to affect a non-federal entity in one or more of the critical infrastructure sectors. The private sector assessment would inform the NCCIC severity rating of a cyber incident.” This assessment process drives many decisions at the national level, including the alert status of the federal government as a whole.

Rather than rely on self-promotional and self-serving private organizations, the HCCIC objectively contextualizes health-centric perspectives, concerns, initiatives, and threats. HHS will leverage and utilize all available DHS cybersecurity support capabilities in its mission to secure healthcare infrastructure. The HCCIC will provide sector-specific context to existing DHS programs such as AIS and will not develop analogous capabilities of any type.

The HCCIC is not a substitute for the NCCIC, and it does not duplicate its mechanisms or operational functionality in any way. The HCCIC is a cybersecurity support appendage to existing emergency response capabilities, and it will both provide the NCCIC with sector-specific knowledge and aid the sector in connecting with the NCCIC and utilizing DHS cybersecurity capabilities.

By nature of the orientation of the public and private sector, DHS and for-profit corporations (which support the ISACs and ISAOs) can never be holistically cooperative. Private entities drive frameworks and policies towards the optimal outcome for their individual organization, while public agencies, like DHS, are tasked with governance and oversight capacities over
multiple sectors. Objective public partners are necessary for the fair and measured improvement in cybersecurity and cyber-hygiene awareness and adoption. The formal and consistent relationship between the NCCIC and a reliable impartial sector-specific agency, like HHS, can best be cemented through open dialogue, transparent intentions, and cooperative initiatives that investigate how sector-specific expertise can be most efficiently leveraged when technical assistance is deployed, rather than wasting valuable resources questioning the validity and intentions of developments, such as the HCCIC, that clearly protect the public and private sector from cyber threats without deliberate bias, fiscal motivations, or obfuscated agendas. Sector-specific expertise unified at the time of government response team deployment, and promulgation of technical assistance lessons learned results in greater critical infrastructure resilience and more effective efforts to mitigate and prevent the impact caused by a cyberattack. For instance, one significant benefit that the HCCIC offers the NCCIC is the incorporation of the existing forensic research and incident reporting capabilities of the HHS Cyber Security Incident Response Center (CSIRC). It provides a sector-level overview and HHS-wide integration to the HHS Health Threat Operations Center (HTOC), which supports real-time information sharing among analysts from HHS, the Defense Health Agency (DHA), and the Veterans Administration (VA).

HHS is developing its cybersecurity mission as a collaboration between the department, DHS, other federal entities, and private sector partners in an attempt to allocate resources effectively to demonstratively increase the security, resiliency, and trust in critical infrastructure systems. Rather than propagating a hollow minimalistic checkbox framework that barely secures vital systems, let alone protects patient data and privacy, HHS is offering a safe, secure, and resilient cyber information sharing environment in the form of the HCCIC, which immediately and impartially disseminates detailed threat indicators while enabling organizations to protect the confidentiality, availability, and integrity of PII and PHI where they are stored, transmitted, or processed without stifling innovation or imposing asymmetric economic barriers. For instance, coalitions of large organizations could standardize or mandate certifications that require resources or expertise unavailable to small and medium-sized entities. An independent agency such as HHS could provide resources and training that SMBs would never receive from market leaders [41].

HHS has three transparent and honest high-level goals for the HCCIC, none of which are redundant to those of the NCCIC. It will strengthen engagement across HHS operating divisions by providing real-time communications among incident response teams and threat analysts across the agency through virtual telecommunications capabilities and physical presence on the HCCIC watch floor. The watch floor allows analysts to evaluate and analyze threats collaboratively in near-real-time, and it facilitates the collocation of analysts and experts from the National Cybersecurity and Communications Integration Center (NCCIC), law enforcement, NH-ISAC, and other federal partners. HCCIC staff is in the process of selecting an analyst portal to boost the watch floor capabilities and provide collaboration opportunities. The portal will
house analysts’ research products to produce HPH-specific bulletins, reports, or newsletters on critical threats, attack vectors, and patterns that include relevant, actionable information such as IP domains and other attributes. The portal will also serve as a code repository for the creation, maintenance, and refinement of analysts’ scripts. HCCIC leadership is working with NH-ISAC to optimize integration with the sector facing portal funded by the ASPR and ONC grants.

The second goal is improved reporting mechanisms and increased awareness of hyper-evolving, healthcare-specific cyber threats achieved by leveraging the HHS enterprise to support the Secretary, ASPR, ONC, and the Office of Security and Strategic Information (OSSI) through coordination of cyber information sharing and to provide a holistic view of HHS cyber operations. Consequently, the HCCIC will provide timely and actionable information, intelligence products, and tactical guidance on threats, vulnerabilities, and risks to organizations less able to ingest and process highly technical data such as the Indicators of Compromise (IOC) provided by the DHS Automated Indicator Sharing (AIS) program and similar private sector products. The final goal is to develop robust public-private partnerships among the federal, private sector, and academic arenas through regular engagement and consistent messaging. HCCIC will continue to interact with the NH-ISAC to support the implementation of the grant awarded by ASPR and ONC, and it will maintain, develop, and promote open communication with all HPH ISAOs in support of the duties of the senior advisor to provide a unified single point of cybersecurity contact for the healthcare sector.

The HCCIC Will Improve Small and Medium-Sized Business’ Access to Threat Data
Companies who participate in information sharing initiatives established through the Cybersecurity Act of 2015 are protected by a liability safe harbor. Nevertheless, many organizations choose not to participate out of legal liability concerns and subjective barriers, such as comparison with competitors and distrust of organizations in individual ISAOs and ISACs. The ISAO and ISAC organizations that claim the HCCIC unnecessary cannot reconcile their opinion with any meaningful justification for their struggle, and often inability, to persuade sector organizations, especially small and medium-sized entities, to share threat information in a timely, standardized, or actionable manner. For instance, the Cybersecurity Act of 2015 established the AIS, a real-time automated system for sharing data. The AIS is a single federal clearinghouse that integrates private sector cyber threat data into the NCCIC. However, it has been difficult to incentivize large organizations to share data through AIS, and it has been complicated to disseminate actionable information to under-resourced small and medium-sized businesses and help them leverage it to prevent, mitigate, and respond to threats. Private sector partners had to be pressured to offer any service to small healthcare providers. They eventually offered a free pared-down version described as “high-tech, low-touch.” Rather than diminish the service and support offered to small organizations who cannot afford to employ seasoned cybersecurity professionals or pay for the assistance of private sector gatekeepers, the proposed
HCCIC will enable and assist struggling small and medium-sized businesses to leverage the NCCIC’s intelligence and services [1].

HCCIC will collaborate with ISAOs and ISACs, but they will Not Dominate It

Select ISAO/ ISAC participants feel disgruntled under the impression that their efforts to comply with DHS guidance and the U.S. government’s drive toward a private sector crowd-sourced cyber-threat sharing ecosystem are left unrewarded. This conclusion is premature and short-sighted. The HCCIC will not eclipse the private sector's vital role in threat sharing; in fact, the HCCIC depends on active, collaborative, and universal private sector participation. However, it will prevent large organizations from asymmetrically receiving all the benefits of information sharing while selectively tailoring their contributions. These jaded, self-serving organizations feel that they answered the government's rallying cry to mitigate emerging threats by sharing information, only to have the rug pulled from their feet. In reality, in their rush to accumulate market power instead of promoting increased sectoral security, large gatekeepers tripped the entire sector and caused its security posture to fall flat. An objective, nonpartisan, and non-profit government entity, such as HHS' HCCIC, is necessary to intermediate between DHS' NCCIC and the healthcare sector. HHS' clearinghouse will provide deep healthcare-centric specialized knowledge to DHS, which the private gatekeepers have failed to supply. Limited membership-based private entities cannot compete with the universal service that the HCCIC will freely provide universally to small, medium-sized, and large sectoral parties [1].

While the HCCIC does need to communicate openly with the private sector on issues such as the roles of the public and private sector in critical infrastructure cybersecurity, no single nebulous private sector center, or multiple varying centers, can match the capability of the federal government in general or HHS’ HCCIC in particular. In just two years under the stewardship of private sector middlemen, the healthcare sector became the number one target of ransomware, APTs, IoT botnets, and other common and even some easily preventable attacks. Arguments that the HCCIC violates some decade-old preconceived role of private sector partners are, from every angle, a self-interested and naïve attempt to maintain influence over the sector after failing to prevent, mitigate, or anticipate every significant cyber-threat of the last few years [1].

The NCCIC May Fail Without the HCCIC

Without the HCCIC, the success of the NCCIC will be dependent on the avarice and will of private companies who are more interested in market incentives than the security posture of the sector [1]. It will not succeed in its mission to secure the HPH sector, because negligent "self-regulating” coalitions of large corporations will institute minimalistic checkbox frameworks that deter liability instead of ensuring security and leverage their status as information gatekeepers against small and mid-size entities. EHRs are universal and transferable within the sector, and systems from all categories of organizations are co-dependent and interconnected. Once struggling SMBs are compromised with ransomware, IoT botnets, or other malware from
cybercriminals, techno-jihadists, Hail Mary threats, digital mercenaries, or advanced persistent threat (APT) groups, large organizations will be laterally compromised and patients will be exploited.
ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg
Sources


[42] Databreaches.net. (2016). *Kaiser notifies 8,000 members whose information was briefly exposed online*. [online] Available at: https://www.databreaches.net/kaiser-notifies-8000-members-whose-information-was-briefly-exposed-online/ [Accessed 12 Jul. 2017].