Journal of Health Care Law and Policy

Volume 21 | Issue 1 Article 3

Cyber-Vulnerabilities & Public Health Emergency Response

Glyn Cashwell

CYBER-VULNERABILITIES & PUBLIC HEALTH EMERGENCY RESPONSE

GLYN CASHWELL, ESQ.

INTRODUCTION

There have been countless large-scale cyberattacks against the health care industry.[1] Failure, degradation, denial-of-service, or integrity issues could significantly hamper public health emergency preparation, response, recovery, and mitigation efforts. Health records are valued at over ten times the amount of credit cards on the black market, and the medical industry is a significant cybersecurity target.[2] Still, the medical industry remains behind most other sectors in its cybersecurity posture.[3] In order to recommend solutions to these problems (I) current cybercrime vulnerabilities and previous attacks should be analyzed; (II) the legal landscape of medical industry cybersecurity should be surveyed; and (III) law and policy recommendations are considered.

I. CYBERSECURITY ATTACKS

Cybercriminals have forged numerous attacks on (A) health networks and devices and (B) the critical infrastructures that countries rely on to prepare for, respond to, recover from, and mitigate the likelihood and probability of public health emergencies.[4]

1. S*ee generally* Kelly Sheridan, *Major Cyberattacks on Healthcare Grew 63% in 2016*, DARKREADNG (Dec. 22, 2016,), http://www.darkreading.com/attacks-breaches/major-cyberattacks-on-healthcare-grew-63—in-2016/d/d-id/1327779 (detailing the increase in cyberattacks on the healthcare industry and vulnerabilities of today's medical devices, patient databases, and healthcare networks).

2. *See* Caroline Humer and Jim Finkle, *Your Medical Record is Worth More to Hackers than Your Credit Card*, REUTERS (Sept. 24, 2014), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

3. John Zorabedian, *Why Cybercriminals Attack Healthcare More Than any Other Industry*, SSOPHOS, (Apr. 26, 2016), http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf.

4. *See generally* Ashley Thomas, *Hack Attack: Cybersecurity Vulnerabilities of Medical Devices*, ABA (Sept. 2015), http://www.americanbar.org/publications/aba_health_esource/2015-2016/september/hackattack.html (explaining the importance of hospitals and health systems improving their infrastructure around healthcare technology).

A. Cyberattacks Directed at Medical Networks or Devices

Health care providers are vulnerable to direct attacks.[5] In 2015, 113 million health care records were breached.[6] Additionally, forty percent of all data breaches in the country in the last three years were associated with the health care industry.[7] Ninety-one percent of medical providers are known cyber-victims.[8] Despite being a major target, "the healthcare industry lags behind other industries when it comes to implementing cybersecurity protections."[9] Health insurance information can be stolen for multiple reasons to include to cover others' medical expenses.[10] Medical records can also contain past payment information such as credit card or checking account information.[11] Aside from using someone else's accounts directly, cybercriminals can also use Personally Identifiable Information (PII) such as social security numbers and dates of birth from health records for identity theft.[12]

Nefarious actors can also exploit individuals' medical diagnoses. For instance, if cybercriminals obtain celebrities' or public figures' medical information during cyberattacks, they could blackmail them.[13] Employers and lenders allegedly purchase medical information for prospective employees and borrowers on the black market.[14] After all, employers might prefer to hire

5. Jim Finkle, *Exclusive: FBI Warns Healthcare Sector Vulnerable to Cyber Attacks*, REUTERS, (Apr. 23, 2014), http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423.

6. HIPAA JOURNAL, *OCR Issues Crosswalk Between NIST Cybersecurity Framework and HIPAA Security Rule*

http://www.hipaajournal.com/ocr-issues-crosswalk-between-nist-cybersecurity-framework-and-hipaa-security-rule-832 (last accessed Nov. 20, 2017).

7. *Id.*

8. Dan Tynan, *Report: Half of U.S. Health Care Providers Have Been Hacked*, YAHOO TECH., (May 7, 2015), https://www.yahoo.com/tech/report-half-of-us-healthcare-providers-have-been-118323228724.html.

9. HIPPA JOURNAL, *supra* note 6.

10. Humer & Finkle, *supra* note 2 (citing a case in which a patient's stolen records were used to cover another person's medical procedure and to purchase medical equipment).

11. *See* Gail Buckner, *Scammers Want Your Medical Records. . .Here's Why*, FOX BUS. (Apr. 14, 2014), http://www.foxbusiness.com/features/2014/04/14/scammers-want-your-medical-recordshere-why.html ("your medical file might also include personal financial information if, for instance, you used your credit card to cover your co-pay.").

12. *See id.*; ERIKA MCCALLISTER, NIST, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (Apr. 2010), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

13. *See* Ariana Eunjung Cha, *Charlie Sheen's HIV Status and the Dawn of Medical-Data Blackmail*, WASH. POST (Nov. 17, 2015), https://www.washingtonpost.com/news/to-your-health/wp/2015/11/17/charlie-sheens-hiv-status-and-the-dawn-of-medical-data-blackmail/ (reporting that Charlie Sheen had been blackmailed for $10 million after his HIV status fell into the hands of criminals).

14. *See* Andrea Peterson, *Privacy Advocates Warn of 'Nightmare' Scenario as Tech Giants Consider Fitness Tracking*, WASH. POST (May 19, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/19/privacy-advocates-warn-of-nightmare-scenario-as-tech-giants-consider-fitness-

employees who do not have medical conditions that might even incidentally affect their work or that might increase a company's medical insurance expenses.[15] Lenders might take medical information into account in determining the likelihood that someone would repay a loan.[16]

Aside from obtaining medical information, hackers can also launch denial-of-service attacks.[17] A large-scale denial-of-service attack would likely require health care providers to modify their standard operating procedures.[18] Such attacks could prevent networked medical devices and equipment from providing status information, resulting in reduced patient care and requiring more workers to measure and report information that would otherwise be available in a centralized location.[19] Not having access to medical records could cause many problems, such as preventing health care staff from being able to access important medical information during a procedure.[20] One hospital had to send patients to other hospitals after ransomware (malware that shuts down a network until funds are paid to a nefarious actor) took down their medical network.[21] Given that many areas of the country are not currently able to meet the "surge capacity benchmark developed by the federal Health Resources and Services Administration" even without large-scale distributed denial-of-service attacks, the impact of these attacks during a widespread health emergency would be disastrous.[22]

Hackers also target medical devices. Medical devices are often integrated within larger networks. This allows nefarious actors who already have infiltrated a medical network to obtain control of the devices if they cannot attack them

tracking/ (discussing fitness application devices could provide employers with access to the private medical data of its employees).

15. *See id.*

16. *See id.* (Explaining how medical information could lead mortgage companies to partake in discriminatory practices).

17. *See* Robert Auger, *Denial-of-Service*, WEB APPLICATION SECURITY CONSORTIUM (Jan. 2010), http://projects.webappsec.org/w/page/13246921/Denial%20of%20Service.

18. *See generally* Sean Gallagher, *Patients Diverted to Other Hospitals after Ransomware Locks Down Key Software*, ARS TECHNICAL (Feb. 17, 2016), http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/ (describing a cyberattack where fetal monitors could not properly record data).

19. Kelly Sheridan *supra* note 1 (detailing the increase in cyberattacks on the healthcare industry and the vulnerabilities in patient databases and healthcare networks).

20. *See id.*

21. *See id.*

22. *See generally* DEREK DELIA, N.J. DEP'T OF HEALTH AND SENIOR SERV., HOSPITAL CAPACITY, PATIENT FLOW, AND EMERGENCY DEPARTMENT USE IN NEW JERSEY (Sept. 2007), http://www.nj.gov/health/rhc/documents/ed_report.pdf (explaining that the surge capacity benchmark is the ability of hospitals to have beds available during periods of high occupancy and citing New Jersey as an example of a state where certain regional hospitals are likely to have a limited number of empty beds relative to the population).

directly.[23] A range of equipment, from monitoring to more critical equipment such as "drug infusion pumps, ventilators and external defibrillators" could be affected.[24] Attacks to some equipment could directly lead to patient injury or death.[25]

Specific cyber-vulnerabilities in a medical setting include (i) personally-owned medical employee devices used to connect to networks that contain PHI and (ii) 'Internet of Things' devices.

i. 'Bring Your Own Device' (BYOD) Security Issues

The cyber-vulnerability to networks at many facilities is exacerbated by the fact that 88% of health care facilities, including hospitals, allow workers to bring their own devices to connect to their network containing PHI to provide patient care.[26] This significantly increases vulnerabilities because health care workers maintain ownership of the device after their shifts.[27] Many Information Technology (IT) departments will not have control, including monitoring and inventorying capabilities, of such devices.[28] Mobile devices that health care workers connect to medical networks with might already contain backdoors or malware. If so, nefarious actors might infiltrate the health care network through workers' mobile devices. IT departments generally have little to no control over personally-owned devices' security configurations, such as antivirus software and encryption settings.[29]

23. *See* David Geer, *The Internet of Things: Top Five Threats to IoT Devices*, CSO (Jan. 9, 2014), http://www.csoonline.com/article/2134265/network-security/the-internet-of-things—top-five-threats-to-iot-devices.html?page=2.

24. *See* Dina Fine Maron, *A New Cyber Concern: Hack Attacks on Medical Devices*, SCI. AM. (June 25, 2013), https://www.scientificamerican.com/article/a-new-cyber-concern-hack (reporting that "the U.S. Department of Homeland Security highlighted one [security] weakness affecting approximately 300 medical devices, included drug infusion pumps, ventilators and external defibrillators").

25. *See id.* (noting that viruses could "render a device unavailable to give care", which could result in risks to patients).

26. *See* PONEMON INSTITUTE, FOURTH ANNUAL BENCHMARK STUDY ON PATIENT PRIVACY & DATA SECURITY 12 (Mar. 2014), https://www.privacyrights.org/sites/privacyrights.org/files/ID%20Experts%204th%20Annual%20Patient%20Privacy%20&%20Data%20Security%20Report%20FINAL.pdf.

27. *See id.* (explaining that most companies do not require security precautions for personal devices).

28. *See id.* (stating that criminal attacks on healthcare systems have increased through use of personal unsecured devices).

29. *See id.* (noting very few employers require employees to have antivirus software on their mobile devices).

ii. 'Internet of Things' Vulnerabilities

Another large problem is that insecure 'Internet of things' devices continue to be added in medical facilities.[30] 'Internet of things' are "smart" devices that connect to networks for remote monitoring and control.[31] 'Internet of things' devices pose serious security risks because security is often not fully considered in early design stages; therefore, many contain known security vulnerabilities that are not patchable.[32] The issue is that 'Internet of things' device manufacturers are generally not incentivized to develop secure devices because the manufacturers need to get products on the market as quickly as possible.[33] Hackers could use well-known vulnerabilities to access such insecure devices as a starting point to infiltrating a larger medical network.[34] Obtaining access to this larger network could allow attackers to obtain large databases of Personal Health Information (PHI).

Many organizations' IT departments do not detect network attacks in a timely manner.[35] Often an attack is not discovered for at least months.[36] As a result, cybercriminals can more easily steal massive amounts of PHI.[37]

B. Infrastructure Cybersecurity Attacks

Two large health care infrastructure dependencies during public health emergencies are (i) the power grid and (ii) telecommunications infrastructure. Both are extremely vulnerable to large-scale cyberattacks.

30. *See* Shaun Sutner, *FDA and UL Weigh In on Security of Medical Devices*, IOT AGENDA (July 2015), http://internetofthingsagenda.techtarget.com/feature/FDA-and-UL-weigh-in-on-security-of-medical-devices-IoT.

31. *See* Jacob Morgan, *A Simple Explanation of 'The Internet Of Things'*, FORBES (May 13, 2014), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#c747a7068284 (explaining such Internet-connected devices include everything from cellphones and wearable devices to coffee makers and washing machines).

32. Bruce Schneier, *The Internet of Things is Wildly Insecure- and Often Unpatchable*, WIRED (Jan. 6, 2014), http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

33. *See id.* at 4 (arguing that the greater rush to put equipment on the market, the more vulnerable the rushed equipment is to viruses and the more difficult it is to patch).

34. *See id.* (noting a large-scale malware hack of 4.5 million users on a common Brazilian DSL router system).

35. *See* Pierluigi Paganini, *Risks and Cyber Threats to the Healthcare Industry*, INFOSEC INST. (Sept. 16, 2014), http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry/ (indicating that 30 million Americans have had their personal health information disclosed as a result of large networks data breeches).

36. *See id.* (stating that many compromised providers were out of compliance because IT staff never detected evidence of attacks on their systems).

37. *See id.*

i. Power Grid Attacks

According to information from Department of Energy, the power grid is hacked several times a week.[38] National Security Agency (NSA) director, Michael Rogers, stated that at least three countries have infiltrated the U.S. power grid.[39] In 2015, a virus called Black Energy took down Ukraine's power grid, leaving 700,000 homes without power.[40] Department of Homeland Security (DHS) analysts revealed that the same virus, Black Energy, "is one of the attack sets periodically found on the U.S. grid."[41] In a recent physical attack in Metcalf, CA, vandals cut major fiber lines and fired multiple rounds into a substation, resulting in $15.4 million of damage to power grid equipment.[42] Former Federal Energy Regulatory Commissioner (FERC), Jon Wellinghoff, stated that if similar attacks were to occur simultaneously in various places throughout the country, they could completely take down the U.S. power grid.[43]

Public health responses are largely dependent on a reliable power grid.[44] After all, most medical equipment requires electricity, and some medications require refrigeration.[45] Because of this, the Department of Health and Human Services (HHS) created a website to assist people who require electricity for treatment or recovery to find places that can continue to supply them power in their area during a large-scale power outage.[46] Although most major care providers have back-up generators and uninterruptible power supplies, these are generally only provided as a stop-gap. Hospitals and other major care providers

38. *See* Steve Reilly, *Bracing for a Big Power Grid Attack: 'One is too Many'*, USA TODAY (Mar. 24, 2015), http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/ ("More often than once a week, the physical and computerized security mechanisms intended to protect Americans from widespread power outages are affected by attacks, with less severe cyberattacks happening even more often.").

39. *See* Katie Bo Williams, *House Energy Bill Boosts Cybersecurity for Electric Grid*, HILL (Dec. 3, 2015), http://thehill.com/policy/cybersecurity/261987-house-energy-overhaul-boosts-grid-cybersecurity; Paul Szoldra, *NSA: It's Only a Matter of Time before Government-Backed Hackers Hit our Power Grid*, TECH. INSIDER (Mar. 1, 2016), http://www.techinsider.io/nsa-chief-infrastructure-2016-3.

40. *See* Szoldra, *supra* note 39 (noting that the attack used malicious software to kill power to these homes); *see also* Paul Szoldra, *The scary-simple way hackers cut electricity to 700,000 homes*, TECH. INSIDER (Jan. 19, 2016), http://www.businessinsider.com/hacker-blackout-ukraine-attack-2016-1 (explaining that 700,000 homes had their power cut).

41. *See* John Quigg, *Ukraine Power Grid Attack Is Wake-Up Call; US Not Ready*, BREAKING DEF. (Jan. 29, 2016), http://breakingdefense.com/2016/01/ukraine-power-grid-attack-is-wake-up-call-us-not-ready/.

42. Reilly, *supra* note 38; Dan Lohrmann, *How Vulnerable Is America's Power Grid?* EMERGENCY MGMT. (May 16, 2014), http://www.emergencymgmt.com/safety/How-Vulnerable-Americas-Power-Grid.html.

43. Lohrmann, *supra* note 42.

44. *See id*. (noting that government response teams are reliant on local power grids).

45. *See id.*

46. Press Release, *HHS launches GIS-based tool for health disaster readiness*, U.S. DEP'T OF HEALTH & HUM. SERVS. (June 23, 2015), http://www.hhs.gov/about/news/2015/06/23/hhs-launches-gis-based-tool-for-health-disaster-readiness.html.

are typically only required by code to have backup power for "functions vital to the protection of life and safety."[47] During Hurricane Sandy, some New York and New Jersey hospitals found their generators were faulty and did not activate during a power outage.[48] The same thing happened in New Orleans hospitals during Hurricane Katrina, and in Connecticut and San Diego in 2011.[49] Furthermore, some generators in older hospitals are in basements, so flooding can damage them.[50] New construction codes require generators to be above flood levels, but these codes do not retroactively apply to older construction.[51]

Larger health provider centers extensively use electronic health records.[52] Reliable power is necessary to access these records.[53] Without access to these electronic medical records, many medical practitioners would have to rely on alternative standard operating procedures such as copious, antiquated hand-written records.[54]

A longer-lasting, widespread power grid outage can also cause an increase in medical emergencies.[55] For instance, more automobile accidents occur when traffic signals are inoperable.[56] Furthermore, those dependent on medical care who require electricity will probably be unable to continue treatments from home.[57] These, along with other indirect problems, could lead to a massive influx of patients that might require hospitals to operate above capacity. If

47. *See* ARCHTOOLBOX, *Emergency and Standby Power Systems for Buildings*, http://www.archtoolbox.com/materials-systems/electrical/emergency-power-systems-for-buildings.html (last visited Apr. 28, 2016); NAT'L FIRE PROT. ASS'N, NFPA 70, NAT'L ELEC. CODE (2005).

48. *See* Charles Ornstein, *Why Do Hospital Generators Keep Failing?* PROPUBLICA (Oct. 31, 2012), https://www.propublica.org/article/why-do-hospitals-generators-keep-failing.

49. *See id.*

50. *See id.*

51. *See id.*

52. *See* NAT'L COORDINATOR FOR HEALTH INFO. TECH., *Hospitals Participating in the CMS EHR Incentive Program* (2015), https://dashboard.healthit.gov/quickstats/pages/FIG-Hospitals-EHR-Incentive-Programs.php (finding that 95% of Eligible and Critical Health hospitals meaningfully use electronic health records).

53. *See, e.g.*, Cheryl Gregg Fahrenholz et al., *Plan B: A Practical Approach to Downtime Planning in Medical Practices*, 80.11 J. OF AHIMA 34 (2009), http://library.ahima.org/doc?oid=95715#.WNw23hiZNsM (explaining how access to electronic health records is essential and describing plans that hospitals can use to continue to operate when they lose power).

54. *See id.* (describing how to transition to a paper process until EHR systems are back online).

55. *See* Chaamala Klinger et al., *Power Outages, Extreme Events and Health: A Systematic Review of the Literature from 2011–2012*, PLOS CURRENTS (Jan. 2, 2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3879211/ (reporting that power outages are associated with extreme events and hospitals see a higher intake of patients during extreme events).

56. *See* Seth Soffian, *Irma Aftermath: Crashes Happen as Drivers Blow Through Inoperable Traffic Lights*, NEWS-PRESS (Sept. 13, 2017), https://www.news-press.com/story/news/2017/09/12/irma-crashes-happening-drivers-blow-through-inoperable-traffic-lights/659688001/.

57. HHS, *supra* note 46.

combined with an imminent public health event, like a bioterrorism attack, the problem would be exacerbated.

ii. Telecommunications Infrastructure

Telecommunications networks are also susceptible to cyberattacks. Many telecommunications networks are dependent on power for continued operations and may be unavailable in a power outage. Telecommunications providers are a prime target for many cybercriminals because they transport massive amounts of sensitive information.[58] Not only can state actors infiltrate telecommunications resources and surveil private communications, they might also incite a large-scale denial-of-service attack.[59] Telecommunications providers have even shut down "critical services" based on false information that an actor had infiltrated parts of their networks.[60] Electronic public health record management is dependent on reliable telecommunications networks, as records should generally be accessible from multiple locations, and information could be stored on the Cloud.[61]

Emergency responders also rely on reliable telecommunications to perform their jobs.[62] People need to be able to reach emergency operators during medical emergencies. Dispatch needs reliable telecommunications to obtain incident information from operators and to allocate resources using a system like Computer-aided Dispatch (CAD).[63] During a larger incident, the incident command post will be located some distance away from the "hot zone" of activity.[64] Adequate telecommunications are necessary for an incident commander to efficiently manage resources. Local and state emergency operating centers, like the Maryland Emergency Management Agency (MEMA), will get involved in large incidents to help effectively use local or state resources

58. *See* DELOITTE, *Global Cyber Executive Briefing: Telecommunications* (2016), https://www2.deloitte.com/global/en/pages/risk/articles/Telecommunications.html (explaining how the telecommunications sector is extremely vulnerable to cyberattacks, while also offering large-scale data and personal information that is valuable for blackmail and resale).

59. *See id.* (explaining that telecom organizations store names, addresses, and financial data).

60. *See id.*

61. Eddie Hooper, *Health Facilities Managements, Open Telecommunications* (May 19, 2015), http://www.hfmmagazine.com/articles/1549-open-telecommunications.

62. *See, e.g.*, Sharoda A. Paul et al., *The Usefulness of Information and Communication Technologies in Crisis Response*, AMIA (2008), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2655958/ (citing an Emergency Department's statement that they received all orders through Internet telecommunications).

63. *See id.* (noting that EMS needs to utilize a technology computer-aided dispatch system that can ensure that all actors have consistent access to accurate information); SUNGARD PUBLIC SECTOR, *Computer Aided Dispatch* (2017), https://www.sungardps.com/solutions/onesolution/public-safety-justice/computer-aided-dispatch/ (explaining that computer-aided dispatch software streamlines communication and increases officer safety).

64. *See* INCIDENT COMMAND POST PROCEDURES (Mar. 2009), http://www.oneonta.edu/admin/police/emergency/erp/07.pdf (describing the factors influencing the location of the Incident Command Post).

in the response and recovery phases of the emergency management cycle.[65] Reliable telecommunications with these agencies and other departments and jurisdictions that form the unified command or unified area command are essential for optimal response.[66]

II. RELEVANT LEGISLATION, REGULATIONS, EXECUTIVE ORDERS (E.O.S), AND PRESIDENTIAL POLICY DIRECTIVES (PPDS)

Because of numerous health care cyberattacks, Congress and the Office of the President have attempted to address the industry's cybersecurity posture. The regulatory landscape includes the (A) Health Insurance Portability and Accountability Act (HIPAA), which was passed in 1996 and emphasizes security planning; (B) Health Information Technology for Economic and Clinical Health (HITECH) Act, which, among other things, extends liability to third parties and incentivizes the use of Electronic Health Records (EHRs); (C) Cybersecurity Act of 2015, which emphasizes information sharing; (D) Health Information Technology: Certification Criteria for Health Information Technology, which provides accreditation standards for Electronic Health Records (EHRs); (E) Cybersecurity Enhancement Act of 2014, which emphasizes information sharing between private companies and the federal government; (F) executive orders that emphasize the importance of critical infrastructure on national security; and (G) Presidential Policy Directives that create task forces and require studies be developed to address critical infrastructure cyber-vulnerabilities.[67] The effectiveness of each will be addressed in turn.

A. Health Insurance Portability and Accountability Act (HIPAA)

The two major components of HIPAA are (i) the privacy rule, which specifies what data should be protected and (ii) the security rule, which dictates the administrative, physical, and technical safeguards that medical practitioners should implement.

65. *See* MARYLAND EMERGENCY MGMT. AGENCY, *About MEMA*, http://mema.maryland.gov/Pages/AboutMEMA.aspx (last visited Jan. 20, 2018) (describing MEMA's work with FEMA to respond to disasters and emergencies occurring in Maryland).

66. *See id.*

67. OFFICE OF PRESS SECRETARY, PRESIDENTIAL POLICY DIRECTIVE, PPD-8, NATIONAL PREPAREDNESS (Mar. 30, 2011); *see also* OFFICE OF PRESS SECRETARY PRESIDENTIAL POLICY DIRECTIVE CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Feb. 12, 2013).

i. Privacy Rule, 45 C.F.R. Parts 160 & 164 (2009)

The HIPAA privacy rule specifies that covered entities need to safeguard Protected Health Information (PHI).[68] PHI is personally identifiable information, such as a name or social security number, that is associated with medical or health information, such as current or previous illnesses, payment information for health care, and medical treatments.[69] Covered entities are health care providers, health plans, or health care clearinghouses (i.e., third parties that deal with formatting non-standard information, such as a third party billing company that determines applicable billing codes before passing information to insurance companies).[70]

ii. Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164 (2009)

HIPAA's security rule addresses various administrative, technical, and physical safeguards to protect data.[71] In order to be flexible, HIPAA security rules have several required protections that must be implemented by every covered entity.[72] Covered entities perform their own self-assessment to determine if each addressable security component is "reasonable and appropriate."[73] If a covered entity determines that an addressable security component is not "reasonable and appropriate," it either documents its rationale in reaching that decision or it implements an "alternative measure."[74] Out of the eighteen HIPAA safeguards, only six are required factors.[75]

Unfortunately for victims of PHI breaches, there is no private cause of action for individuals under HIPAA for an individual to obtain a remedy from harm caused by a covered entity's HIPAA breach (note, however, that, as discussed later, HITECH allows state attorney generals to bring causes of action for HIPAA violations on behalf state residents).[76] In other words, a private

68. *See* HHS, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (2010), http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

69. *See id.*

70. *See* 45 CFR § 160.103 (2013); HHS, *Covered Entities and Business Associates*, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Apr. 28, 2016).

71. *See* HHS, *Summary of the HIPAA Security Rule*, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (last visited Apr. 28, 2016).

72. *See id.*

73. *See id.*

74. *See* DEP'T. HEALTH & HUM. SERVS SUMMARY OF THE HIPAA SECURITY RULE (last visited Apr. 28, 2016), http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/.

75. *HIPAA Security Series: 1 Security 101 for Covered Entities;* DEP'T. HEALTH & HUM. SERVS., 10–11 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (revised Mar. 2007).

76. *I.S. v. Wash. Univ.*, No. 4:11CV235SNLJ, slip op. at 1 (E.D. Mo. June 14, 2011); *see also Legal Alert: HIPAA May Provide Basis for State Law Private Cause of Action*, MCGUIREWOODS (June 23, 2011), https://www.mcguirewoods.com/Client-Resources/Alerts/2011/6/HIPAA-May-Provide-Basis-

individual cannot bring a civil action against a covered entity under HIPAA for HIPAA violations.[77] An individual may have other causes of action that can be brought under other laws, like state negligence claims. In negligence cases, a violation of HIPAA might be used as evidence to help show the relevant standard of care and not being HIPAA-compliant might be evidence of the breach of that standard of care.[78] Even though private citizens can file complaints to the Office of Civil Rights (OCR) within HHS, OCR is responsible for levying fines upon covered entities that violate the statute.[79]

Some security advocates are worried that covered entities are so concerned with ensuring they are HIPAA-compliant that they do not have funding and resources to implement other security controls that could be more effective against medical identity theft.[80] Security expert Reece Hirsch with Morgan, Lewis, & Bockius concludes that "mere compliance with the HIPAA Security Rule is not sufficient if current cyber risks are not being taken into account."[81]

B. Health Information Technology for Economic and Clinical Health (HITECH) Act

The HITECH Act extends HIPAA requirements and liability to include business associates in addition to covered entities.[82] Business associates are third parties that implement various solutions on behalf of covered entities.[83]

The HITECH ACT also encourages covered entities to develop Electronic Health Records (EHRs).[84] The U.S. government believed EHRs would reduce

for-State-Law-Private-Cause-of-Action.aspx ("HIPAA does not create a private right of action, under federal law.").

77. *See* Kane Russell, Coleman Logan PC, *Is There a Private Cause of Action for HIPPA Violations?*, LEXOLOGY (Jan. 28, 2016), https://www.lexology.com/library/detail.aspx?g=a5bc1a0f-557a-4bf1-8cd3-1498c872a4dc.

78. *See id.*

79. *See HIPAA What to Expect*, DEP'T. HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/filing-a-complaint/what-to-expect/index.html; *Cignet Health Fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations*, DEP'T. HEALTH & HUM. SERVS. (Apr. 11, 2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/index.html?language=es (describing how HHS fined Cignet health $4.3 million for HIPAA privacy rule violations).

80. *See* Bob Violino, *7 Ways to Work Around Security Compliance Problems*, CSO (Jan. 6, 2014), http://www.csoonline.com/article/2134254/it-audit/7-ways-to-work-around-security-compliance-problems.html ("the misunderstanding related to HIPAA can have a negative impact on certain business processes, affect application performance and even cause users to bypass certain controls because they're annoyed at security").

81. Beth Walsh, *Top Legal Issues in Healthcare Include Cybersecurity, HIPAA, Telemedicine*, CLIN. INNOVATION + TECH. (Feb. 10, 2016), http://www.clinical-innovation.com/topics/ehr-emr/top-legal-issues-healthcare-include-cybersecurity-hipaa-telemedicine.

82. 42 U.S.C. § 17931 (2012).

83. *See id.*; HHS, *supra* note 68.

84. *See id.*

health care costs and improve care.[85] EHRs have the potential to prevent duplicative tests and allow medical providers to transfer records between each other to obtain a more wholistic picture of patients' conditions.[86] The government initially provided covered entities with incentive payments if they "meaningfully" used certified EHRs in their practice.[87] Now providers that do not "meaningfully use" EHR systems must pay the government a percentage of their Medicare/Medicaid revenues.[88]

The Office of the National Coordinator for Health Information Technology (ONCHIT) delegates its responsibility to certify EHRs to third parties.[89] This certification process does not appear to be rigorous, as many certified EHRs have serious usability and security issues.[90] As a result, many argue HITECH has largely failed to meet its goal of providing a more effective, efficient system of records.[91]

The EHR incentive/penalty program may have incentivized covered entities to convert to EHRs quickly without covered entities fully considering applicable safeguards that should be put in place as part of EHR implementation.[92] By doing so, appropriate safeguards were not designed into some EHR systems from the initial design development stage.[93] Adding technical security safeguards after the final design stage is typically extremely expensive, ineffective, and can make the entire system bulkier and less user-

85. *Benefits of Electronic Health Records (EHRs)*, HEALTHIT.GOV (last updated Jul. 30, 2015), https://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs (Jul. 30, 2015); *see also* Sue Bowman, *Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications*, PERSP. HEALTH INFO. MGMT. (Oct. 1, 2013), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3797550/.

86. *See Health Information Exchange (HIE): What is HIE?*, HEALTHIT.GOV https://www.healthit.gov/providers-professionals/health-information-exchange/what-hie, (May 12, 2014) (discussing health information exchanges set up to exchange EHR between physicians, leading to benefits including reduced duplicative testing).

87. *See* HHS, *Meaningful Use Regulations*, https://www.healthit.gov/policy-researchers-implementers/meaningful-use-regulations (last visited Apr. 28, 2016).

88. *See id.*

89. *See* HHS, *About the ONC Health ITSec Health IT Certification Program* (2016), https://www.healthit.gov/policy-researchers-implementers/about-onc-health-it-certification-program.

90. *See* David Blumenthal, *Stimulating the Adoption of Health Information Technology*, 360 NEW ENG. J. MED. 1477, 1479 (Aprtl, 9, 2009) (noting that many certified EHRs are neither user-friendly nor designed to meet quality and efficiency standards.).

91. *Id.*

92. *Id.*

93. *See* Joseph Goedert, *Encryption Remains Afterthought for Meaningful Use*, HEALTH DATA MGMT. (Oct. 8, 2015), htttps://www.healthdatamanagement.com/news/encryption-remains-afterthought-for-meaningful-use (stating that HITECH failure to mandate encryption lead to security concerns); *see also* Joe Marion, *Granting Access: An EHR Security Risk?* HEALTHCARE INFORMATICS (June. 1, 2009), http://www.healthcare-informatics.com/blogs/jlmblog/granting-access-ehr-security-risk (noting that cardiovascular patient information EHR database did not have privacy safeguards designed into its system when developed).

friendly.[94] The cost of redesigning an EHR system to address security flaws can be cost-prohibitive.[95]

The HITECH Act provides a potential way for patients harmed by a covered entity's violation of HIPAA to recover. However, it only allows a state's attorney general to bring class action suits on behalf of patients in the state.[96] Therefore, it still limits the ability of patients to recover from harm caused by covered entities' HIPAA violations.

The HITECH Act also does not require covered entities or business associates to report a lost or stolen device to HHS if data was encrypted by an approved encryption algorithm.[97] Encrypting mobile devices with an algorithm accepted by OCR, therefore, can save covered entities large sums of money in fines or related lawsuits.[98]

C. Cybersecurity Act of 2015

The Cybersecurity Act consists of (i) general provisions that apply to additional industries besides health care and (ii) provisions that are specific to the health care industry.

i. General Provisions

The Cybersecurity Act of 2015, also referred to as the Cybersecurity Information Sharing Act (CISA), primarily focuses on the ability of private entities to share cyber-threat information with the government.[99] The act was a response to the large Office of Personnel Management (OPM) data breach, and

94. *See* Ann Cavoukian and Richard C. Alvarez, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win*, INFORMATION AND PRIVACY COMMISSIONER (Mar. 2, 2012), https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-ehr-e_1.pdf (noting the advantages of embedding privacy as a first consideration of EHR systems).

95. *See How Much is This Going to Cost Me*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/faqs/how-much-going-cost-me (last visited Apr. 17, 2016) (noting the high cost of redesigning, purchasing, and installing an EHR system).

96. *See* Health Information Technology for Clinical and Economic Health Act Pub. L. No. 111-5, 123 Stat. 225, 279 (2009); Barbara Fox, *Mobile Medical Apps: Where Health and Internet Privacy Law Meet*, 14 HOUS. J. HEALTH L. & POL'Y 193, 215 (2014).

97. *See* Office of Civil Rights, *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

98. *See* Mike Semel, *HIPAA Doesn't Require Data Encryption, but you Should*, 4MEDAPPROVED, (Feb. 4, 2013), http://www.4medapproved.com/hitsecurity/hipaa-data-encryption/ ("The HITECH Act of 2009 modified the HIPAA data breach rule by stating that if a device is lost or stolen, the loss is not reportable as a HIPAA data breach if the data is encrypted in compliance with data encryption guidance from the National Institute of Standards and Technology (NIST).").

99. *See* Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 29 Stat. 694, 694–744 (2015); Suz Redfearn, *Einstein Efforts Accelerate Under the Spotlight of OPM Breach*, FED. TIMES (Aug. 10, 2015), http://www.federaltimes.com/story/government/cybersecurity/2015/08/10/opm-breach-kick-starts-einstein-efforts/31424351/.

it designates DHS as the government point of contact for information sharing with the private sector.[100] Businesses are required "to use technical means" to scrub personally identifiable information before it is transferred to DHS.[101]

Despite the safeguards that DHS applies to the data, privacy advocates are concerned that the statute enables the government to spy on U.S. citizens.[102] Businesses are not given incentives to ensure that personal information is correctly scrubbed from the data forwarded to DHS as businesses are relieved from liability by showing that the information they sent was "directly related and necessary" to assess a cybersecurity threat.[103] Some have argued that the act's overall effect will be to infringe on citizens' privacy rights without providing security mechanisms to prevent harm to citizens from data breaches because this "directly related and necessary" standard is vague.[104] The government argues that the act allows them to better provide businesses with information about how they can secure data and provide effective security solutions.[105]

Personal Health Information that entities share with DHS could contain particularly private information. Citizens are concerned that covered entities and business associates that share such information with DHS might not adequately remove personally identifiable information or that DHS could use data mining techniques to uncover the identities associated with underlying health information.[106] Furthermore, citizens question how well the government safeguards personal information after the OPM breach.[107] If DHS were to handle citizens' personal health information in a similar manner that OPM handled its data, DHS could be indirectly responsible for medical identity theft. By even

100. Cybersecurity Information Sharing Act of 2015, *supra* note 99; Paul Rosenzweig, *The Cybersecurity Act of 2015*, LAWFARE (Dec. 16, 2015), https://www.lawfareblog.com/cybersecurity-act-2015.

101. Rosenzweig, *supra* note 100.

102. LETTER FROM CIVIL SOCIETY ORGANIZATIONS TO CONGRESS (Dec. 17, 2015), http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/12-17-15%20Coalition%20Letter%20to%20Members%20of%20Congress%20urging%20opposition%20to%20the%20Cybersecurity%20Act%20of%202015.pdf.

103. Jadzia Butler, *CISA's Interim Guidelines: A Good Start, but with Lingering Privacy Concerns*, CTR. FOR DEMOCRACY & TECH. (Feb. 26, 2016), https://cdt.org/blog/cisas-interim-guidelines-a-good-start-but-with-lingering-privacy-concerns/.

104. *Id*.

105. *See* Lauren Walker, *Senate Passes Controversial CISA Bill Letting Companies Share Cybersecurity Information with Government*, NEWSWEEK (Oct. 27, 2015), http://www.newsweek.com/senate-passes-controversial-cisa-bill-companies-share-cyber-security-387785 (noting that by allowing the sharing of information, the government will be able to better coordinate with private companies and improve cyberattack responses).

106. Butler, *supra* note 103.

107. *See* Zachary Figueroa, *Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for Centralized Cybersecurity Infrastructure*, 24 CATHOLIC U. J. L. & TECH 433, 434 (2016), *available at* https://scholarship.law.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1016&context=jlt.

obtaining and storing such information, DHS may become a big cyber target. If cyber-threat data is not properly handled and stored securely, citizens' information might be more vulnerable to cybercriminals than ever before.

ii. Health Care-Specific Provisions

The Cybersecurity Act of 2015 has three health care-specific provisions.[108] The first provision provides that cyber-threat information be shared with entities across the health care industry. Such sharing should be especially beneficial to smaller providers.[109] Second, the act defines the cybersecurity roles and responsibilities of each HHS department.[110] It creates a HHS task force to identify common cyber-threats in the health care sector and to incorporate best practices from other industries.[111] Third, it mandates that HHS create cybersecurity guidelines for covered entities and business associates.[112] How helpful these guidelines could be to smaller providers will ultimately depend on the usability of the information provided to practitioners. If the guidelines specify automated programs that providers with limited technical capabilities can install and utilize, then they may be very useful. Unfortunately, a lot of the information that agencies have provided in the past is abstract because it also must be flexible. For instance, National Institute of Standards and Technology's cybersecurity framework only provides references to bulky standards to implement various security components.[113] HHS's "Guide to Privacy and Security of Public Health Information" contains a cybersecurity section, but it does not recommend architectures or specific technology.[114] HHS's cybersecurity website focuses on developing security plans and risk assessments.[115] HHS's "Top 10 Tips for Cybersecurity in Health Care" is a step in the right direction, but even that references unwieldy standards such as National Institute of Standards and Technology (NIST) "Special Publication 800-88, Guidelines for Media Sanitation" and uses terminology that many non-technical workers would probably not understand.[116] HHS's cyber-attack

108. *See* Marianne Kolbasuk McGee, *Analysis: Cybersecurity Law's Impact on Healthcare: HIMSS Legislative Expert Outlines Key Provisions and Their Implications*, GOVINFOSECURITY (Dec. 22, 2015), http://www.govinfosecurity.com/interviews/analysis-cybersecurity-laws-impact-on-healthcare-i-3027.

109. *See id.*

110. *See id.*

111. *See id.*

112. *See id.*

113. *See* NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

114. ONCHIT, GUIDE TO PRIVACY AND SECURITY OF ELECTRONIC HEALTH INFORMATION, 30 (Apr. 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

115. *See id.*

116. *See* NIST, SPECIAL PUBLICATION 800–88, GUIDELINES FOR MEDIA SANITIZATION (Dec. 2014), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf; HHS, *Top 10 Tips for Cybersecurity in Health Care* (Jan. 12, 2015).

checklist contains guidance that even non-technical professionals should be able to comprehend and implement, but this is mostly useful only if an attack has actually been discovered and only after an attack has occurred.[117] HHS should focus on providing specific technical guidance in terms non-technical people can understand to properly address cyber-threats beyond the requirements to simply comply with HIPAA.

D. HHS, Health Information Technology: Certification Criteria for Health Information Technology (45 CFR Part 170, Subpart C)

HHS, "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology" specifies EHR certification criteria.[118] Specific requirements include authentication, access control, laboratory test result integration, audit logs, emergency access, and electronic interfaces to allow for communication with public health departments.[119]

The final rule for EHR Incentive Program for Stage 3 only mentioned that encryption should be included in risk analyses. Therefore, the government does not mandate EHR encryption.[120] The rule also requires administrative and physical safeguards that are already required under HIPAA.[121]

The Final Rules for 2015 Edition Health IT Certification Criteria explicitly addressed requirements to improve interoperability of EHR systems to provide better exchange of information with other providers and with patients.[122]

E. Executive Order (E.O.s) 13010 and 13636: Critical Infrastructure Security

Executive Orders (E.O.s) 13010 and 13636 highlight the importance of critical infrastructure to national security.[123] E.O. 13010 creates a President's Commission on Critical Infrastructure Protection and identifies cyber-threats to the country's infrastructure. That order emphasizes critical infrastructure's role in maintaining economic prosperity and national security.[124] President Obama reemphasized the importance of securing critical infrastructure in E.O. 13636.[125]

117. *See, My Entity Just Experienced a Cyber-Attack! What Do we Do Now?*, U.S. DEP'T OF HEALTH & HUM. SERVS (June 2017), https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf.

118. *See* 42 CFR § 412, 42 CFR § 495.

119. *Id.*

120. *Id.*

121. *Id.*

122. *See CMS FACT SHEET: EHR Incentive Programs in 2015 and Beyond*, CMS (Oct. 6, 2015), https://www.cms.gov/Newsroom/MediaReleaseDatabase/Fact-sheets/2015-Fact-sheets-items/2015-10-06-2.html.

123. *See* Exec. Order No. 13,636, 3 C.F.R. 13636 (2013).

124. *See* Exec. Order No. 13,010, 3 C.F.R. 13010 (1996), *available at* https://www.gpo.gov/fdsys/pkg/CFR-1997-title3-vol1/pdf/CFR-1997-title3-vol1-eo13010.pdf.

125. Exec. Order No. 13,636, *supra*, note 123.

That order promotes cybersecurity information sharing between private and public sectors, orders the government to create a cybersecurity framework for critical infrastructure, and calls for incentives to critical infrastructure providers that promote robust cybersecurity practices.

Both (a) NIST's *Framework for Improving Critical Infrastructure Cybersecurity* and (b) DHS's *Cybersecurity Evaluation Tool* came out of these executive orders.[126]

i. National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity

NIST's Framework for Improving Critical Infrastructure Cybersecurity is a good first step in identifying relevant standards for defensive cybersecurity measures in various sectors.[127] It provides standards that can be used by any critical infrastructure industry.[128] The government does not mandate that critical infrastructure providers comply with the framework, and it provides companies with extensive flexibility in determining how to implement security solutions.[129] At the same time, the framework does not identify specific example solutions or architectures that providers could implement.[130]

The government created a crosswalk to map parts of HIPAA's security rule to the NIST Cybersecurity Framework to assist the health care industry in complying with both.[131] Covered entities will still have to expend significant effort to determine how to implement technical cybersecurity measures based on bulky standards set by the crosswalk lists.[132] After all, instead of providing detailed examples of technical solutions to consider, the crosswalk contains references to HIPAA and general standards.[133]

ii. DHS Cybersecurity Evaluation Tool

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides assessments for critical infrastructure services at no charge.[134] It also provides a Cybersecurity Evaluation Tool.[135] The tool is focused on helping an organization develop a security plan and identify vulnerabilities

126. *Id.*; Exec. Order No. 13,010, *supra*, note 124.

127. HIPPA JOURNAL, *supra* note 6.

128. *See* Cybersecurity Enhancement Act of 2014, S. 1353, 113th Cong. (2014), *available at* https://www.govtrack.us/congress/bills/113/s1353; NIST, *supra* note 113.

129. Cybersecurity Information Sharing Act of 2015, *supra* note 99; NIST, *supra* note 116.

130. *Id.*

131. HIPAA JOURNAL, *supra* note 6.

132. *Id.*

133. *Id.*

134. *See* DHS, ASSESSMENTS, https://ics-cert.us-cert.gov/Assessments (last visited Apr. 29, 2016).

135. *See id.*

instead of suggesting specific technical security solutions.[136] For instance, the tool assists users in documenting their network configurations, in obtaining a listing of general security standards, in reviewing administrative safeguards, and in performing a risk assessment.[137]

F. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274: Voluntary Public-private Partnership for Cybersecurity

The Cybersecurity Enhancement Act of 2014 calls for National Institute of Standards and Technology (NIST) to develop "standards and procedures to cost-effectively reduce cyber risks to critical infrastructure."[138] This was largely implemented in NIST's "Framework for Improving Critical Infrastructure Cybersecurity" that was also required by Executive Order (E.O.) 13636.[139]

The Cybersecurity Enhancement Act of 2014 also called for specific government departments to create cybersecurity research and development plans.[140] Under this approach, both HHS and Department of Energy (DoE), in collaboration with NIST, are responsible for creating cybersecurity plans every four years.[141] The act also calls for the government to incentivize cybersecurity education by granting scholarships and for NIST to develop cybersecurity training programs.[142]

G. Presidential Policy Directive 8 (PPD-8) and 21 (PPD-21)

Presidential Policy Directives 8 and 21 identify cybersecurity threats to critical infrastructure as national security vulnerabilities that must be addressed.

PPD-8 called for a Strategic National Risk Assessment (SNRA), which considered the most pertinent natural, cyber, terrorist, and health emergency threats.[143] The SNRA determines which threats pose the largest risks and provides preparation, response, mitigation, and recovery recommendations for these national threats.[144] Most of the SNRA results are classified because there are security concerns that adversaries could use SNRA information to forge a

136. *See* DHS, *Cybersecurity Evaluation Tool*, https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf (last visited Apr. 29, 2016).

137. *See id.*

138. Cybersecurity Information Sharing Act of 2015, *supra* note 99.

139. Cybersecurity Information Sharing Act of 2015, *supra* note 99; NIST, *supra* note 116.

140. Cybersecurity Information Sharing Act of 2015, *supra* note 99.

141. *Id.*

142. *Id.*

143. *See* DHS, THE STRATEGIC NATIONAL RISK ASSESSMENT IN SUPPORT OF PPD 8: A COMPREHENSIVE RISK-BASED APPROACH TOWARD A SECURE AND RESILIENT NATION (Dec. 2011), https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

144. *See id.*

more successful attack against the nation.[145] However, general information from the SNRA is available to the public.[146] The President mandated that the SNRA be created in order to define a National Preparedness Goal.

PPD-21 focuses on the importance of infrastructure security to the overall security of the country and recommends an all-hazards approach to ensure critical infrastructure resiliency.[147] PPD-21 recommends emergency managers consider degraded power grid conditions and communication systems during planning processes.[148] President Obama dictated that these recommendations should be included in an updated National Infrastructure Protection Plan.[149] PPD-21 also promotes mechanisms for private entities to share situational awareness information with the federal government.[150] In order for the government to assess information from infrastructure providers, PPD-21 calls for a "system-of-systems" evaluation to analyze the dependencies critical infrastructure systems have on each other and on national security.[151]

III. RECOMMENDATIONS

The current regulations, laws, PPDs, and EOs are insufficient to avert numerous successful cybersecurity attacks. In particular the laws, regulations, PPDs, and EOs do not generally provide enough incentives for providers to improve their cybersecurity posture. The following recommendations would address this: (A) the EHR accreditation process should include rigorous security and interoperability scrutiny; (B) HHS should modify their regulatory approach to increase the number of required security rule safeguards and to provide covered entities/business associates incentives to improve their cybersecurity posture; and (C) emergency management should become more integrated with the cybersecurity community.

A. EHR Accreditation Should Involve More Security and Interoperability Scrutiny

Because most EHRs have numerous cyber-vulnerabilities, ONCHIT should increase the rigor its third parties apply in their "meaningful use" EHR accreditations. This can be accomplished by ensuring specific security controls are implemented- not just considered in a risk assessment.

145. *See id.*

146. *See id.*

147. *See* CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, Presidential Policy Directive No. 21 (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

148. *See id.*

149. *See id.*

150. *See id.*

151. *See id.*

ONCHIT should require that organizations implement essential security safeguards in their EHR systems.[152] Many accredited systems do not contain sufficient security controls or meet usability standards.[153] ONCHIT should verify that the user's authentication, accounting, and authorization system is set up, there are mechanisms for data integrity, and that data is adequately encrypted.[154] ONCHIT should also ensure that pertinent physical security measures are implemented.[155] An example of a physical security measure is controlling physical access to critical servers that contain information protected by the privacy rule.[156] ONCHIT should also ensure that there are mechanisms in place to prevent employees from downloading large datasets of PHI that they then could, either intentionally or inadvertently, provide to adversaries.

ONCHIT should also provide more scrutiny during usability tests. ONCHIT should consider creating a certification checklist that adequately represents functionality that EHR systems should contain. The fact that so many systems have been accredited that lack basic usability and interoperability standards is an embarrassment. Initially, it might cost more to adopt thorough accreditation processes. However, the potential to automate EHR testing could decrease long-term costs and meet the goals of HITECH. ONCHIT is trying to address these interoperability issues by working with industry to develop and improve standards and has developed an interoperability roadmap, but there is still significant work before EHR systems truly interoperate with one another.[157]

B. Modify Law and Regulatory Framework to Provide Covered Entities and Business Associates with Incentives to Better Secure their Systems

HIPAA provides health care providers flexibility in allowing them to determine if business considerations warrant addressing many security safeguards. At the same time, HIPAA does not allow for a private cause of action

152. *Medicare and Medicaid Programs*, *supra* note 118.

153. *See* Bowman, *supra* note 85; Blumenthal, *supra* note 90.

154. *Medicare and Medicaid Programs*, *supra* note 118.

155. *Id.*

156. *Id.*

157. *See* Robert H. Dolin et al., *Setting the Standard: EHR Quality Reporting Rises in Prominence Due to Meaningful Use*, J. OF AHIMA 85 (Jan. 2014), http://library.ahima.org/doc?oid=300255 ("To determine quality of care, one must analyze end-to-end EHR processes—from data capture at the point of care to electronic reporting—and the role of standardized data in determining quality of care. The Centers for Medicare and Medicaid Services (CMS) has been taking a leadership role in the promotion of the use of standards through an open process that engages measure developers, clinician users, EHR vendors, professional societies, and other key stakeholders… Such standards are a prerequisite for EHR functionality and are a foundational component of the strategy for quality reporting from EHRs. CMS, recognizing this foundational role, has taken a leadership position as evidenced through their sponsorship of several key initiatives, including standards development and convening a multi-stakeholder collaboration to improve these standards."); ONCHIT, *Connecting Health and Care for the Nation*, https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf.

when covered entities and business associates inadequately protect PHI (note, however, that, as discussed above, HITECH allows for the state attorney general to bring a cause of action under HIPAA on behalf of state's' residents). Currently there are two primary options for those harmed by a HIPAA violation to recover: (1) use the entity's breach of the HIPAA security rule to show a breach of duty in a "negligence per se" or other tort state claim, as supported by *I.S. v. Washington Univ.* or (2) request that the state attorney general institute a class action on behalf of the state's citizens, but the state attorney general retains discretion over whether to bring the suit.[158] Note, however, that courts are not bound by *I.S. v. Washington Univ.* for PHI breach negligence per se cases, as it was decided at the district court level, and it was only a decision to not dismiss and to remand to state court, as the cause of action was a state "negligence per se" claim.[159]

Continued large data breaches, especially by insurance companies, imply that the fact that there is no private cause of action under HIPAA for breaches does not provide a significant incentive for covered entities and business associates to appropriately safeguard PHI.[160] In addition to focusing on whether a covered entity has created a security plan and considered addressable issues, laws should also probably require that ONCHIT or another agency provide more clear-cut security requirements and regulations that can be updated regularly. Specific changes to the current regulatory framework that could improve health cybersecurity include (i) banning medical practitioners from allowing employees to connect directly to networks containing PHI; (ii) scrutinizing 'Internet of things' (IoT) devices and IoT settings; (iii) requiring encryption whenever entities handle or transmit patient data; (iv) allowing for a private cause of action with a presumption of causation in data breaches cases; (v) providing security rankings for covered entities and business associates; (vi) disseminating and encouraging use of automated security test tools; and (vii) discouraging collection of non-pertinent patient information.

i. HHS Should Ban 'Bring Your Own Device' (BYOD) Models

HHS should ban employees from using their own devices, versus those owned and managed by a medical facility's IT department, to access networks that contain PHI. 88% of health care organizations permit employees to use their own mobile devices to access health care networks that might contain PHI, and

158. *I.S. v. Washington Univ.*, *supra* note 76; *see also* MCGUIREWOODS, *supra* note 76; Fox, *supra* note 96.

159. *Id.*

160. *See* Elise Viebeck, *Regulator Dings Premera over Breach Notification Wait*, HILL (Mar. 17, 2015), http://thehill.com/policy/cybersecurity/236002-regulator-dings-premera-over-breach-notification-wait; Michael Hiltzik, *Anthem is Warning Consumers about its Huge Data Breach. Here's a Translation*, LA TIMES (Mar. 6, 2015), http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html#page=1.

many of these covered entities do not seem to appreciate the risks associated with their BYOD policies.[161] Compounding the problem, many mobile applications that employees load on their mobile devices can also leak PHI from the health network.[162]

The biggest problem with allowing employees to access health networks with their own devices is accountability. Health care administrators typically will not be able to access an employee's mobile device after he or she has left the facility. Administrators might not be able to ensure that employees' mobile devices incorporate the most up-to-date security updates, incorporate encryption capabilities, or contain authentication, auditing, and authorization capabilities. If an employee's non-password-protected device contains PHI and it is subsequently stolen, a nefarious actor could obtain and illicitly use that PHI. Even with password protection, administrators cannot ensure that information stored on employees' mobile devices is encrypted. As a result, a cybercriminal might be able to obtain information from an unencrypted hard drive on a password-protected device. Criminals can break weak passwords with dictionary or brute force attacks.[163] These attack programs are "widely available tools that utilize wordlists and smart rulesets to intelligently and automatically guess user passwords."[164] Even worse, all of this could occur without the IT administrator's knowledge. After all, employees are generally unlikely to report thefts of personally-owned mobile device to their employers' system administrators.

At least when IT administrators maintain control of mobile devices, they can require accountability for lost devices, disable USB ports to prevent employees from transferring data stores of PHI and other information, control the applications that are installed on devices, ensure that data is encrypted both

161. *See* PONEMON INSTITUTE, FOURTH ANNUAL BENCHMARK STUDY ON PATIENT PRIVACY & DATA SECURITY 12 (Mar. 2014), https://www.privacyrights.org/sites/privacyrights.org/files/ID%20Experts%204th%20Annual%20Patient%20Privacy%20&%20Data%20Security%20Report%20FINAL.pdf ("The BYOD usage continues to rise despite the concerns about employee negligence and the lack of security for mobile devices. Nearly 88 percent of organizations permit medical staff to use their own mobile devices to access their organization's networks and services like email. The most worrying aspect is that nearly 50 percent of organizations are not aware of the risks related to BYOD, and only a limited portion of organizations require their employees to adopt proper countermeasures like anti-malware.").

162. Lisa Phifer, *Leaky Enterprise: Data Loss Tops Mobile Security Threats*, TECHTARGET, http://searchsecurity.techtarget.com/feature/Leaky-enterprise-Data-loss-tops-mobile-security-threats (last visited Apr. 29, 2016) (According to Michael Raggo, director of security research at MobileIron and co-author of Data Hiding, "'Our research shows that even legitimate apps can expose PII [personally identifiable information] or PHI [protected health information] by embedding libraries that have some sort of adware or data harvesting capability.'").

163. *See* Chris Hoffman, *Brute-Force Attacks Explained: How All Encryption is Vulnerable*, HOW TO GEEK (July 6, 2013), http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/.

164. *See* Mark Burnett, *Blocking Brute Force Attacks*, UVA (2007), https://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php.

when it is at rest and when it is being transmitted over networks, and require that passwords meet security requirements.

ii. Regulatory Framework Should Scrutinize 'Internet of Things' Devices

'Internet of Things' (IoT) devices are notorious for having excessive security vulnerabilities because many of the products were not designed with security in mind.[165] Many also do not even provide adequate security patches for known vulnerabilities.[166] IoT devices that do not contain adequate security controls can be vulnerable to direct attacks. These device attacks can cause them to not operate as intended, and patient injury or death may result.[167] IoT devices are also susceptible to denial-of-service attacks, rendering devices unavailable when needed.[168]

The 'Internet of things' offers many benefits.[169] For instance, maintenance, monitoring, and status information can often be relayed to a centralized IT system and to appropriate parties.[170] These benefits can help automate health care by allowing the aggregation of information from disparate devices onto a single display and providing opportunities for improvements in health care by alerting staff to anomalous patient conditions quickly.[171] Network administrators, however, should be extremely cautious about integrating 'Internet of things' devices into their networks if the devices are insecure. 'Internet of things' devices may offer cybercriminals an insecure node that can be used to infiltrate the rest of the network and obtain critical PHI.[172]

HHS should consider providing security ratings and important patching information for 'Internet of things' devices that are commonly used in the medical field. The FBI recommends that IT administrators ensure IoT device default passwords are changed to strong passwords, Universal Plug and Play Support on network devices are disabled, and IoT devices are put on their own enclave, which is a protected network set off from other networks using a firewall.[173]

165. Schneier, *supra* note 32.

166. *Id.*

167. *Id.*

168. *Id.*

169. Morgan, *supra* note 31.

170. *Id.*

171. *Id.*

172. Schneier, *supra* note 32.

173. *See* Erin McCann, *FBI Issues Alert for IoT Device Security*, HEALTHCARE IT NEWS (Sept. 16, 2015), http://www.healthcareitnews.com/news/fbi-issues-alert-iot-device-security ("The FBI offered a list of recommendations. 1. Keep up-to-date with security patches for these devices. 2. Ditch any default passwords you may still have and make them stronger: 'Do not use the default password determined by the device manufacturer,' since many can be found online. 3. Disable UPnP on routers 4. Isolate IoT devices on their own protected networks.").

iii. Encryption Requirements Should Be Required Under HIPAA and for EHR Accreditation

At a minimum, covered entities and business associates should encrypt all PHI before transmitting or storing it. The "eMedicare and Medicaid Electronic Health Records (EHRs) Incentive Program; Stage 3 and Modifications to Meaningful Use in 2015 through 2017" specifies that encryption should be considered in a risk analysis, but it does not require EHR systems to implement encryption for accreditation.[174] The fact that encryption was not an EHR requirement was mentioned in official comments to the EHR Incentive Program rule, and CMS responded by stating that it was not going to add an encryption requirement to the rule.[175]

iv. Injured Parties Should Be Allowed to Bring Private Causes of Action Under HIPAA

Allowing private causes of action under HIPAA for PHI breaches in addition to allowing a state attorney general to bring them 'might provide monetary incentives for covered entities and business associates to provide more rigorous security precautions. Patients sometimes cannot recover in a negligence claim from a PHI breach because they cannot show that a particular defendant was responsible for the data breach that caused their medical identity to be stolen.[176] For instance, the harm a plaintiff suffered could have been caused by a data breach by numerous other actors other than the defendant.[177] In *Kahle v. Litton Loan Servicing, LP*, the plaintiff's negligence action alleged that Litton negligently stored hard drives containing customer personal information that were later stolen.[178] The Court dismissed the lawsuit, holding that plaintiff could not establish proximate cause because

> even if Kahle had established that the unauthorized use of her personal information had occurred following the theft. . ., her claims would have failed because she could not have established that Litton's alleged actions were the proximate cause of the unauthorized use of information. Like many consumers, Kahle disclosed her personal information to third parties on a regular basis.[179]

174. *See Meaningful Use Definition & Objectives*, HHS (Feb. 6, 2015), https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives; *Medicare and Medicaid Programs*, *supra* note 118.

175. *Medicare and Medicaid Programs*, *supra* note 118.

176. *See* Jonah Comstock, *What the New HIPAA Means for Digital Health Access*, MOBIHEALTHNEWS (Jan. 28, 2013), http://mobihealthnews.com/20039/what-the-new-hipaa-means-for-digital-health-access.

177. *See id.*

178. 486 F. Supp. 2d 705, 706-07 (S.D. Ohio 2007).

179. R. Bruce Allensworth et al., *Recent Federal Court Decision Bolsters Growing Line of Cases Dismissing Class Action Claims for Alleged "Identity Theft,"* K&L GATES (July 26, 2007), http://www.klgates.com/recent-federal-court-decision-bolsters-growing-line-of-cases-dismissing-class-

Furthermore, in some courts, plaintiffs cannot recover simply because their data was breached in a negligence action as they must show "injury-in-fact." In *Ruiz v. Gap*, a cybercriminal stole two laptops and obtained sensitive information for approximately 750,000 prior job applicants.[180] That information included applicants' mothers' maiden names, drivers' license numbers, and social security numbers.[181] In that case, the court held that data breach victims did not show all elements of a negligence claim because divulging personal information, without associated monetary loss, did not amount to an "injury-in-fact."[182] Similarly, the plaintiff's contract claim for breach of the privacy policy failed because he could not show economic loss due to that breach.[183]

Clapper v. Amnesty International USA held that to "establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'"[184] A circuit split has emerged in applying *Clapper* to data breach cases with some circuits finding that plaintiffs have standing solely by alleging their information was stolen and with other circuits requiring plaintiffs to allege more particularized injuries associated with the breach of their information to have standing.[185]

If an individual direct cause of action under HIPAA were permitted under law and if courts did not require proof that a patient suffered harm from PHI theft from the negligence of a specific covered entity or business associate, then it would alleviate a significant burden from plaintiffs in the current legal data breach patchwork (i.e., standing and the injury/causation elements in a negligence case).[186]

Another option is to allow plaintiffs that suffered harm from medical identity theft to have a rebuttable presumption in a negligence action that a company that had a disclosed data breach that included the plaintiff's medical information is responsible for at least a certain amount of nominal harm resulting

action-claims-for-alleged-identity-theft-07-26-2007/; *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705, 706-07 (S.D. Ohio 2007).

180. *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 910 (N.D. Cal. 2009) aff'd, 380 F. App'x 689 (9th Cir. 2010).

181. *See id.*

182. *See id.*

183. *See id.*

184. *Clapper v. Amnesty Int'l USA*, 548 U.S. 398 (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U. S. 139, 140 (2010) (slip op., at 7)).

185. *See* Sean McIntyre, *Deeper Dive: Clapper Divide Expands In Data Breach Cases*, DATA PRIVACY MONITOR (June 13, 2017), https://www.dataprivacymonitor.com/privacy-litigation/deeper-dive-clapper-divide-expands-in-data-breach-cases/.

186. Comstock, *supra* note 176 ("I know there have been a couple of class action suits filed, but that law is not at present well developed in terms of the private right of individuals whose private health information has been disclosed. And the issue there is 'What's the damage?' You have to show damage, and it's very nebulous.").

from their information being breached. Covered entities and business associates should only be able to overcome this presumption by showing that they complied with reasonable cybersecurity safeguards. Such a scheme would likely incentivize covered entities and business associates to promulgate stricter security rules to prevent successful lawsuits against them.

Covered entities and business associates will probably argue that a private right of action with a rebuttable presumption against them could result in medical doctors and insurance companies leaving the field because of increased liability. Also, they could argue that allowing for a private right of action would increase health care costs for everyone. However, the burden of the cost in the current framework is on patients who are ill-equipped to protect themselves- both financially and because they generally have little to no control over how health care companies secure their PHI.

v. HHS Should Provide Security Ratings for Covered Entities and Business Associates

HHS should provide security ratings for business associates that provide underlying technical security controls for covered entities. This would allow covered entities to better determine the level of security they are getting from providers and analyze that against the cost for services. Specifically, rating cloud computing options could be very beneficial to covered entities who use a cloud computing architecture because "more than 13% of cloud services used in the healthcare industry are considered high–risk; 77% are at medium risk."[187] ONCHIT provides a list of accredited EHR products.[188] If EHR systems were also rated based on cybersecurity capabilities, covered entities could make better, more informed decisions when selecting EHR systems.

Also, HIPAA should consider rating covered entities and publishing such information. With a simple A-F cybersecurity rating mechanism, consumers could take cybersecurity information into account when selecting medical providers or health plans. The federal government could require that covered entities and business associates post their cybersecurity rating both on company websites and in conspicuous locations in health care facilities. If cybersecurity proves to be a major concern for many patients, such a rating system might incentivize covered entities and business associates to improve their security posture. Without such knowledge in the current environment, there is decreased incentive for covered entities and business associates to fund cybersecurity measures.

187. Paganini, *supra* note 35.

188. *See* ONCHIT, *Comprehensive List of Certified Health Information Technology*, http://oncchpl.force.com/ehrcert (last visited Apr. 29, 2016).

vi. HHS Should Provide Basic Automated Security Testing and Penetration Tools to Covered Entities and Business Associates

If HHS is not already doing so, it should provide some form of automated testing and penetration tools to covered entities and business associates. Such automated testing should be user-friendly and require as little technical knowledge as possible to decrease technical costs to health care providers. Such automated testing should also provide detailed implementation information about how to fix identified security issues. The provided penetration tools should probably not be any more sophisticated than free penetration tools available online in order to prevent illicit use of such tools by nefarious actors.

If not already a part of HHS's cybersecurity alerts, HHS might also consider creating a more sophisticated automated test suite or penetration tools that the government could run to alert covered entities/business entities of known security vulnerabilities. HHS might want to consider including such test suites as part of ONCHIT's EHR accreditation process. These more complex tools should probably not be provided to covered entities or business associates if those tools could be used by cybercriminals to more effectively hack networks.

vii. Regulations to Reducing Unnecessary Data Collection Could Improve Security

Medical providers might be able to reduce the harm caused by PHI theft by reducing the amount of unnecessary personally identifiable data collected and stored by EHRs. In particular, covered entities could stop making it a practice to require patients to disclose their social security number or date of birth. Also, although it might be possibly more challenging administratively, medical providers could make it a practice to not store patient bank account and credit card information for future use.

C. Involve Cybersecurity Elements and Infrastructure in Emergency Planning Efforts

Emergency planners should consider emergency situations where basic infrastructure, such as the power grid or telecommunications equipment, is unavailable.[189] PPD-21 specifically requires emergency managers to plan for a power grid outage.[190] Many covered entities already have several forms of mitigation, such as backup power supplies and generators. During a massive public health emergency; however, hospitals can be beyond surge capacity and such mitigation measures might not be enough to address many patients'

189. Fahrenholz et al., *supra* note 53.

190. *See* Critical Infrastructure Security and Resilience, *supra* note 147.

needs.[191] As part of this planning effort, cybersecurity experts, utilities, and telecommunications operators should help in providing insight. Because telecommunications, utilities, and covered entities are typically privately owned, it is sometimes difficult to get input from such stakeholders. The government should incentivize these private companies to participate in such planning as much as possible to provide optimal solutions.

In order to optimally utilize resources in emergency planning efforts, the government should (1) provide first responders with meaningful cybersecurity training that they can use in planning with private infrastructure companies and (2) declassify relevant portions of the SNRA and similar documents that local emergency responders could use in planning for all four stages of the emergency management cycle.

i. Federal and Local Governments Should Provide More Appropriate Cybersecurity Training to Emergency Responders

Having FEMA develop meaningful cybersecurity training for emergency managers might enable them to better prepare for, mitigate from, respond to, and recover from an emergency brought on by a cybersecurity attack. In FEMA's National Response Report, emergency managers have consistently ranked cybersecurity as the core capability that needs most improvement.[192] Some viable cyberattack planning considerations could be identified at the federal level and promulgated to local emergency managers. The government should help the public respond to and recover from attacks to critical infrastructure. Cities should consider alternative ways that citizens can contact first responders during a major telecommunications outage and options that they have in the event of a power grid emergency. Emergency managers should develop alternative operating procedures for use during critical infrastructure outages and should consider the special needs of disabled citizens or those with medical equipment that relies on electricity.

191. DELIA, supra note 22 at x ("On 47 days in 2005, more than 95% of all maintained beds in the state were occupied. This number increased from 29 days in 2004 and 11 days in 2003. On these days, there would be almost no immediate surge capacity available to respond to a major emergency such as a natural disaster or terrorist attack without displacing existing patients. On more than ¾ of the days in 2003 through 2005, the state had less than 500 empty staffed beds available per million residents, which is a surge capacity benchmark developed by the federal Health Resources and Services Administration.").

192. *See* DHS, NATIONAL PREPAREDNESS REPORT (Mar. 30, 2015), http://www.fema.gov/media-library-data/1432751954859-fcaf2acc365b5a7213a38bbeb5cd1d61/2015_NPR_508c_20150527_Final.pdf.

ii. The Government Should Declassify Additional Portions of SNRA and Similar Documents, as Applicable, to Share with Emergency Responders, Public Health Officials, and Health Care Providers

Considering the extensive resources that went into developing the SNRA, it would be helpful to declassify information derived from that study that could help emergency managers in planning for critical infrastructure outages.[193] Obviously, such information should only be declassified to the extent that it would not damage national security by providing salient information about the country's weaknesses to adversaries. Because the SNRA includes inputs from multiple high-level officials, it may be a strong starting point for emergency managers in developing local plans for related emergencies.[194]

IV. CONCLUSION

Cybercriminals will continue to attack the country's medical infrastructure unless cybersecurity regulations and policies are updated. New legislation and regulations should focus on providing covered entities and private critical infrastructure companies with incentives to create secure and resilient networks. Unfortunately, people whose medical information is stolen suffer most from these attacks, and typically they are the most ill equipped to recover from them. Currently, the government does not provide consumers with the information necessary to select covered entities or business associates based on their cybersecurity posture. Therefore, future legislation and regulation should focus on providing cybersecurity information to consumers, incentivizing better security practices, and planning emergency management efforts for large-scale cybersecurity attacks.

193. *See* DHS, THE STRATEGIC NATIONAL RISK ASSESSMENT IN SUPPORT OF PPD 8: A COMPREHENSIVE RISK-BASED APPROACH TOWARD A SECURE AND RESILIENT NATION 1 (Dec. 2011), http://www.fema.gov/media-library-data/20130726-1854-25045-5035/rma_strategic_national_risk_assessment_ppd8_1_.pdf ("As part of the effort to develop the National Preparedness Goal and identify core capabilities, the Secretary of Homeland Security led an effort to conduct a strategic national risk assessment to help identify the types of incidents that pose the greatest threat to the Nation's homeland security. Representatives from the offices of the Director of National Intelligence and the Attorney General, as well as other members of the Federal interagency, supported this effort.").

194. *Id.*