UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 4 Article 13

Spring 2015

'The Greatest Wealth is Health': Patient Protected Health Information in the Hands of Hackers, 31 J. Marshall J. Info. Tech. & Privacy L. 657 (2015)

Samantha Singer

COMMENT

'THE GREATEST WEALTH IS HEALTH': PATIENT PROTECTED HEALTH INFORMATION IN THE HANDS OF HACKERS

SAMANTHA SINGER*

INTRODUCTION

From April to June 2014, "4.5 million patients" of 206 Community Health Systems' hospitals, operating out of 29 different states, had their personal information stolen including "names, Social Security numbers, addresses," birthdays, and telephone numbers as a result of a Chinese 'cyber-attack' on their protected health information ("PHI").[1] This cyber-attack was conducted by bypassing the hospitals' security systems[2] using "high-end, sophisticated malware."[3] Prior to this attack 204 similar attacks were reported in 2014 alone.[4]

As technology becomes more integrated into society there has been a shift away from traditional "hard-copy" health records and a shift to-

---

* Samantha Singer received her BA in Political Science with a concentration in Criminal Justice from Oakland University in 2012. Currently, Samantha is pursuing her Juris Doctor at The John Marshall Law School, expected May 2016. Comment title: *Quoting*, Publius Vergillius Maro "Virgil" ancient Roman poet: *Quotes to Make you feel better*, CBHS *available at* http://cbhs.com.au/whats-new/latest-news/quotes-to-make-you-feel-better.aspx (last visited Nov. 19, 2014).

1. Nicole Perlroth, *Hack of Community Health Systems Affects 4.5 Million Patients*, THE N. Y. TIMES (Aug. 18, 2014, 3:39 PM), http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/?_php=true&_type=blogs&_r=0.

2. *Id.*

3. *Hackers Steal 4.5 Million Patient Records from Multi-State Hospital Network*, RT USA (Aug. 18, 2014), http://rt.com/usa/181172-chs-hospital-network-hacked/.

4.Andrew Towle, *Hacking Into Cash Flow*, GUARDIAN LIBERTY VOICE (Aug. 21, 2014), http://guardianlv.com/2014/08/hacking-into-cash-flow/.

wards electronic health records ("EHR"),[5] resulting in patients' PHI being at a greater risk of being hacked into, sold on the black market, and/or used by individuals other than the patient and their medical providers. The major contributor to this shift towards electronic medical records ("EMR")[6] is the Health Information Technology for Economic and Clinical Heath Act ("HITECH"),[7] which is a section of the American Recovery and Reinvestment Act of 2009.[8] The HITECH Act required, that as of "January 1, 2014 all public and private healthcare providers and other eligible professionals ("EP") must have adopted and demonstrated a 'meaningful use' of electronic medical records ("EMR") in order to maintain their existing Medicare and Medicaid reimbursement levels."[9]

One of the core values of the EMR program is to "protect patients' privacy and security" with regard to their PHI.[10] To achieve its goal the EMR program breaks down the meaningful use requirement into three different stages over a five-year period, from 2011-2016.[11] The three

---

5. Electronic health record (EHR) is defined by HealthIT.gov as "a digital version of a patient's paper chart." *What is an electronic health record (EHR)?*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-ehr (last updated Mar. 16, 2013). Additionally, EHR is described as being, "real-time, patient-centered records that make information available instantly and securely to authorized users." *Id.*

6. Similarly to EHR, EMR "is a digital version of a paper chart," however, EMR only "contains all of the patient's medical history from one practice." *Benefits of EHRs: What is an Electronic Medical Record (EMR)?*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/electronic-medical-records-emr (last updated Aug. 29, 2014). Therefore, EMR is a compilation of "the standard medical and clinical data gathered in one provider's office," while EHR is a collection of data from multiple providers and "include[s] a more comprehensive patient history." *Id.*

7. *American Recovery and Reinvestment Act of 2009*, H.R. 1, 111th Cong. § 13001(a) H.R. 1-112 (2009)(enacted) *available at* http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf.

8. *What is the HITECH Act & What Does it Mean to Eligible Providers?* CAL-MED (2010), http://www.cal-med.com/Stimulus.aspx (last visited Sept. 28, 2014). Beyond the HITECH Act many States, such as Massachusetts, Minnesota, and Maryland are beginning to "mandate … physicians to show they know how to use an EHR by 2015 or face the loss of their license to practice..." Ken Terry, *State EHR Mandates*, PHYSICIANS PRACTICE (Aug. 18, 2010) (on file with author).

9. University Alliance, *Federal Mandates for Healthcare: Digital Record-Keeping Will Be Required of Public and Private Healthcare Providers, USF HEALTH* (Feb. 8, 2013), http://www.usfhealthonline.com/news/healthcare/electronic-medical-records-mandate-january-2014/#.VAzMg0sk0aA.

10. Guide to Privacy and Security of Health Information, THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. 28 (1.2st ed. 2012) (on file with author).

11. *EHR Incentives & Certification: How to Attain Meaningful Use*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/how-attain-meaningful-use (last updated Jan. 15, 2013).

stages include, "Stage 1, data capturing and sharing" to be implemented in 2011-2012; "Stage 2, advance clinical processes" to be implemented in 2014; and "Stage 3, improved outcomes" to be implemented in 2016.[12]

Unfortunately, as a result of EHR vendors and EPs/eligible hospitals ("EHs") creating and implementing EHR technology that complies with the three stages of meaningful use, patients' privacy and security has been put at risk. From the creation of the HITECH Act in 2009 to 2013 there has been "804 large breaches of protected health information ("PHI") affecting over 29.2 million patient records."[13] In 2012-2013 alone there was a 137.7% increase in the number of breaches of patients' PHI reported.[14] Therefore, in order to combat the number of security breaches and privacy issues resulting from EHR technology, EHR vendors and EPs/EHs must do something beyond what is currently required, to improve patients' privacy and security.

This comment will analyze the specific requirements and stages that EPs/EHs must comply with in order to receive its Medicare and Medicaid incentives, how EHR technologies are being implemented, how EHR technologies are affecting patients' privacy with regard to hacking a patient's PHI, and what EHR technology vendors and EPs/EHs should be doing to improve patient privacy and security to prevent hacking and other breaches.

Part I of this comment will address hacking of PHI. Part II will analyze the security measures that EHR vendors must currently incorporate into EHR technology and how the lack of required security measures impacts patients' privacy and security. Part III discusses the security measures EPs/EHs are implementing in order to successfully achieve the three meaningful use requirements and analyzes how patients' PHI is being put at risk and Part IV examines the consequences of EP/EHs' non-compliance with HIPAA Privacy and Security Rules. Finally, Part V will propose a solution, requiring EHR vendors to incorporate HIPAA compliant security measures into their technology, implementing HIPAA certification programs that EHR technology trainers must obtain prior to training EPs/EHs on EHR technology, and requiring continuing education for EPs/EHs specifically regarding the improvement of patients' security.

BACKGROUND

Within the United States Constitution the Fourth Amendment pro-

12. *Id.*

13. *Breach Report 2013: Protected Health Information (PHI)* 3 (2014), *available at* https://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf.

14. *Id.*

tects individuals' rights to privacy by stating:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[15]

In order to determine whether or not a person's medical information is protected by the Constitution the Supreme Court in *Whalen v. Roe* stated that protecting privacy has at least two different interests: (1) "individual interest in avoiding disclosure of personal matters;" and (2) "the interest in independence in making certain kinds of important decisions."[16] Taking into consideration these two different interests, the Court has held that medical records fall within the scope of the first privacy protection interest and there is a limited privacy right afforded to an individual's medical records.[17]

Therefore, in order to create "a national framework for security standards and protection of confidentiality with regard to health care data and information"[18] Congress passed the Health Insurance Portability and Accountability Act ("HIPAA") of 1996.[19] Congress' main goal when enacting HIPAA was to protect the "privacy and security of individually identifiable health information…whether the information is on a computer, paper, or other media."[20] To achieve this goal HIPAA's "regulations" were broken down into three different categories: (1) "administrative simplification… creat[ing] uniform standards and requirements for the electronic transmission of health information;" (2) "privacy… set[ting] forth general rules for the use and disclosures of individually identifiable health information;" and (3) "security…requir[ing] providers…to maintain the security and integrity of individually identifiable health information."[21]

The HIPAA Privacy Rule which was enacted on December 28, 2000,[22] applies to PHI in any medium[23] and establishes "national stand-

---

15. U.S. CONST. amend. IV.

16. *Whalen v. Roe,* 429 U.S. 589, 598-600 (1977).

17. *Doe v. Southeastern Pa. Transp. Auth.,* 72 F.3d 1133, 1137 (3d Cir. 1995).

18. *Health Insurance Portability and Accountability Act (HIPAA)*, NY STATE OFFICE OF MENTAL HEALTH, https://www.omh.ny.gov/omhweb/hipaa/ (last updated Nov. 15, 2012).

19. *Id.*

20. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 28.

21. NY STATE OFFICE OF MENTAL HEALTH, *supra* note 18.

22. *Health Information Privacy: The Privacy Rule*, U.S. DEPT. OF HEALTH & HUMAN SERV., http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ (last visited Nov. 8, 2014).

ards to protect individuals' medical records and other personal health information … [by requiring] appropriate safeguards to protect the privacy of personal health information, and [setting] limits and conditions on the uses and disclosures that may be made of such information without patient authorization."[24] Additionally, the HIPAA Privacy Rule "gives patient[']s rights over their health information," by allowing patients "to examine and obtain a copy of their health records, and to request corrections."[25]

Alternatively, the HIPAA Security Rule, finalized on February 20, 2003, creates "national standards to protect individuals' electronic personal health information [e-PHI] that is created, received, used, or maintained by a covered entity."[26] The HIPAA Security Rule requires that covered entities "conduct risk analysis to identify risks and vulnerabilities" to e-PHI.[27] Additionally, the HIPAA Security Rule requires the implementation of policies and procedures to "prevent, detect, contain, and correct security violations by conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the organization."[28] These requirements are carried out by requiring EPs/EHs to train their staff on what is expected of them, including, how to implement the policies and procedures in order to maintain patient privacy protections, consistently utilizing the provider's policies and procedures when a breach occurs, periodically reviewing and revising policies to insure they are up-to-date and being implemented properly.[29] In addition the requirements also provide that EPs/EHs review and revise policies when there is an internal or external change in the practice, and that EPs/EHs "retain policies and procedures for six years" after the policies have been updated or replaced.[30]

---

23. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 28. Any medium includes, "electronic, oral, or paper." *What Health Information Is Protected by the Privacy Rule?*, U.S. DEPT. OF HEALTH & HUMAN SERV. NATIONAL INST. OF HEALTH, http://privacyruleandresearch.nih.gov/pr_07.asp (last updated Feb. 2, 2007).

24. *Health Information Privacy: The Privacy Rule*, *supra* note 22.

25. *Id.*

26 *Health Information Privacy: The Privacy Rule*, *supra* note 22. Covered entities include "health plans, health care clearinghouses, health care providers who conduct certain financial and administrative transactions electronically." *Who Must Comply With HIPAA Privacy Standards*, HHS.gov (Dec. 19, 2002 *updated* Nov. 9, 2006) http://www.hhs.gov/ocr/privacy/hipaa/faq/covered_entities/190.html.

27. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 10.

28. *Id.* (*Quoting* The HIPAA Privacy Rule, Administrative Safeguards, 45 CFR § 164.308 (2013)).

29. *Id.* at 22-23.

30. *Id.* at 22-23.

On February 17, 2009, Congress enacted the HITECH Act as a section of the American Recovery and Reinvestment Act of 2009.[31] The HITECH Act was passed in order to "promote the adoption and 'meaningful use' of health information technology."[32] Additionally, the HITECH Act Subtitle D, Privacy,[33] addresses privacy and security concerns with regard to e-PHI, as well as incorporating and expanding upon the HIPAA Security Rules.[34]

In order to implement the HITECH Act's provisions for adoption and meaningful use, in 2011,[35] Medicare and Medicaid began offering the Medicare and Medicaid Electronic Health Records ("EHR") Incentive Program.[36] This program provides monetary incentives to EPs, such as, "Doctors of Medicine or Osteopathy, Doctors of Dental Surgery or Dental Medicine, Doctors of Podiatric Medicine, Doctors of Optometry, and Chiropractors" and EHs, such as, "hospitals in the 50 states or DC that are paid under the hospital inpatient prospective payment system, critical access hospitals ("CAHs"), Medicare Advantage Affiliated Hospitals (MA-Affiliated Hospitals), Acute Care Hospitals with at least ten percent Medicaid patient volume, cancer hospitals, and Children's Hospitals," as long as they are capable of demonstrating "adoption, implementation, upgrading, or meaningful use of certified EHR technology."[37] Additionally, this program defines meaningful use as, "using certified electronic health record ("EHR") technology to: (1) improve quality, safety, efficiency, and reduce health disparities; (2) engage patients and family; (3) improve care coordination, and population and public health; and (4) maintain privacy and security of patient health information."[38]

The Medicare and Medicaid EHR program then broke down the

---

31. *HITECH Act Enforcement Interim Final Rule*, U.S. DEPT. OF HEALTH & HUMAN SERV., http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (last visited Sept. 28, 2014).

32. *Id.*

33. *American Recovery and Reinvestment Act of 2009*, H.R. 1, 111th Cong. H.R. 1-144 (2009)(enacted) *available at* https://epic.org/privacy/pdf/StimulusPassedBill-SubD.pdf.

34. *HITECH Act Enforcement Interim Final Rule*, *supra* note 31.

35. *Medicare and Medicaid EHR Incentive Program Basics*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html (last updated Feb. 18, 2015).

36. *Welcome to the Medicare & Medicaid EHR Incentive Program Registration & Attestation System*, CENTERS FOR MEDICARE & MEDICAID SERV., https://ehrincentives.cms.gov/hitech/login.action (last visited Sept. 28, 2014).

37. *Id.*

38. *EHR Incentives & Certification- Meaningful Use Definition & Objectives*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives (last updated Feb. 6, 2015).

definition of meaningful use even further by separating it into three specific components. The three components of meaningful use are: (1) the "use of certified EHR in a meaningful manner;" (2) the "use of certified EHR technology for electronic exchange of health information to improve quality of health care;" and (3) the "use of certified EHR technology to submit clinical quality measures and other measures selected by the Secretary."[39] For EPs and EHs to comply with the meaningful use components, the components were broken down into three different stages: "Stage 1, data capturing and sharing; Stage 2, advance clinical processes; and Stage 3, improving outcomes," to be completed over a period of five years, from 2011-2016.[40]

Stage 1, data capturing and sharing, which was implemented in 2011-2012, required EPs and EHs to meet certain objectives in order to obtain incentive payments.[41] During Stage 1, EPs had to meet 13 core objectives, 5 out of 9 menu set objectives,[42] and 9 clinical quality

---

39. *Medicare & Medicaid EHR Incentive Program: Meaningful Use Stage 1 Requirements Overview*, CENTERS FOR MEDICARE & MEDICAID SERV. 3, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/MU_Stage1_ReqOverview.pdf (last visited Sept. 28, 2014).

40. *EHR Incentives & Certification*, *supra* note 11.

41. *Id.*

42. *2014 Definition Stage 1 of Meaningful Use*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html (last updated Oct. 6, 2014).

> EP's Core Objectives include:
>
> (1) CPOE [computerized provider order entry]; (2) [implementing] drug-drug and drug-allergy interaction checks; (3) [maintaining] an up-to-date problem list of current and active diagnoses; (4) [generating] and [transmitting] permissible prescriptions electronically (eRx); (5) [maintaining] active medication list; (6) [maintaining] active medication allergy list; (7) [recording] … demographics [including]: (A) preferred language; (B) gender; (C) race; (D) ethnicity; (E) date of birth; (8) [recording] and [charting] changes in …vital signs…; (9) [recording] smoking for patients 13 years old or older; (10) [implementing] one clinical support rule related to a high priority hospital condition along with the ability to track compliance with that rule; (11) [providing] patients the ability to view online, download, and transmit information about a hospital admission; (12) [providing] clinical summaries for patients for each office visit; and (13) [protecting] electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
>
> *Eligible Professional Meaningful Use Table of Contents Core and Menu Set Objectives*, EHR INCENTIVE PROGRAM, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EP_MU_TableOfContents.pdf (last visited Nov. 8, 2014).
>
> EP's Menu Set Objectives include:

measures.[43] EHs had to meet 11 core objectives, 5 out of 10 menu set objectives,[44] and 16 clinical quality measures.[45] Clinical quality

---

(1) [implementing] drug formulary checks; (2) [incorporating] clinical lab-test results into EHR as structured data; (3) [generating] lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, or outreach; (4) [sending] patient reminders per patient preference for preventive/follow-up care; (5) [using] certified EHR technology to identify patient-specific educational resources and provide those resources to the patient if appropriate; (6) the EP who receives a patient from another setting of care or provider of care or believes an encounter is relevant should perform medication reconciliation; (7) the EP who transitions their patient to another setting of care or provider of care or refers their patient to another provider of care should provide summary care record for each transition of care or referral; (8) capability to submit electronic data to immunization registries or immunization information systems and actual submission according to applicable law and practice; and (9) capability to submit electronic syndromic surveillance data to public health agencies and actual submission according to applicable law and practice.

Id.

43. *2014 Clinical Quality Measures*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/2014_ClinicalQualityMeasures.html (last updated July 22, 2014).

44. *2014 Definition Stage 1 of Meaningful Use*, *supra* note 41.

EH's Core Objectives include:

(1) CPOE; (2) [implementing] drug-drug and drug-allergy interaction checks; (3) [maintaining] an up-to-date problem list of current and active diagnoses; (4) [maintaining] active medication list; (5) [maintaining] active medication allergy list; (6) [recording] … demographics [including]: (A) preferred language; (B) gender; (C) race; (D) ethnicity; (E) date of birth; (F) date and preliminary cause of death in the event of mortality in the eligible hospital…; (7) [recording] and [charting] changes in …vital signs…; (8) [recording] smoking for patients 13 years old or older; (9) [implementing] one clinical support rule related to a high priority hospital condition along with the ability to track compliance with that rule; (10) [providing] patients the ability to view online, download, and transmit information about a hospital admission; and (11) [protecting] electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Eligible Hospital and CAH Meaningful Use Table of Contents Core and Menu Set Objectives, EHR INVENTIVE PROGRAM, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EH_CAH_MU_TableOfContents.pdf (last visited Nov. 8, 2014).

EH's Menu Set Objectives include:

(1) [implementing] drug formulary checks; (2) [recording] advance directives for patient[s] 65 years old or older; (3) [incorporating] clinical lab-test results into EHR as structured data; (4) [generating] lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, or outreach; (5) [using] certified EHR technology to identify patient-specific educational resources and provide those resources to the patient if appropriate; (6) the eligible hospital… who receives a patient from another setting of care or provider of care or be-

measures were required to be reported on in order for an EP/EH to comply with the meaningful use requirements and to receive Medicare/Medicaid incentive payments.[46] This is because the clinical quality measures are used to "measure or quantify healthcare processes, outcomes, patient perceptions, and organizational structure and/or systems that are associated with the ability to provide high-quality health care and/or relate to one or more quality goals for health care… [including] effective, safe, efficient, patient-centered, equitable, and timely care."[47]

"Stage 2, advance clinical processes," is to be reported on in 2014 and requires EPs and EHs to meet similar objectives to Stage 1 prior to obtaining incentive payments.[48] To achieve Stage 2 incentives EPs must report on 17 core objectives and 3 of 6 menu objectives.[49] While, EHs must demonstrate 16 core objectives and 3 of 6 menu objectives.[50]

"Stage 3, improving outcomes," is to be reported by 2016.[51] Unfortunately, the requirements for Stage 3 are still being considered and therefore are not available at this time.[52]

Beyond the core objectives, menu objectives, and clinical quality measures EPs/EHs continue to have the duty to insure the privacy and security of its EHR programs. Although there are a multitude of EHR

> lieves an encounter is relevant should perform medication reconciliation; (7) the eligible hospital… that transitions their patient to another setting of care or provider of care or refers their patient to another provider of care should provide summary care record for each transition of care or referral; (8) capability to submit electronic data to immunization registries or immunization information systems and actual submission according to applicable law and practice; (9) capability to submit electronic data on reportable…lab results to public health agencies and actual submission according to applicable law and practice; and (10) capability to submit electronic syndromic surveillance data to public health agencies and actual submission according to applicable law and practice.

Id.

45. *2014 Clinical Quality Measures*, CMS.GOV, *supra* note 43.

46. *EHR Incentives & Certification*, *supra* note 11.

47. *Quality Measures*, CMS.GOV, http://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/QualityMeasures/index.html?redirect=/qualitymeasures/03_electronicspecifications.asp (last visited Nov. 8, 2014).

48. *EHR Incentives & Certification*, *supra* note 11.

49. *Eligible Professional's Guide to Stage 2 of the EHR Incentive Programs*, CENTERS FOR MEDICARE & MEDICAID SERV. 6 (Sept. 2013), http://www.cms.gov/Regulations-and Guidance/legislation/EHRIncentivePrograms/Downloads/Stage2_Guide_EPs_9_23_13.pdf.

50. *Stage 2*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Stage_2.html (last updated Nov. 5, 2014).

51. *EHR Incentives & Certification*, *supra* note 11.

52. Anthony Brino, *Stage 3 MU Now in the Making*, HEALTHCARE IT NEWS (Feb. 10, 2014), http://www.healthcareitnews.com/news/stage-3-mu-now-making.

technology vendors, the EP/EH, not the EHR vendor is responsible for implanting policies and procedures that "protect the confidentiality, integrity, and availability of health information" as well as continuing to "comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules."[53] This is because EHR technology vendors are not required to make their products compliant with HIPAA Privacy and Security Rules, leaving a great burden solely on EPs/EHs to protect their patients' PHI.[54]

In order to comply with HIPAA Privacy and Security Rules as well as the meaningful use requirements, it is virtually impossible to have an EHR technology that does not require an internet connection.[55] This is because within the core objectives of meaningful use, EPs and EHs are required to be able to, for example, "generate and transmit permissible prescriptions electronically (eRx)" or "provide patients the ability to view online, download, and transmit information about a hospital admission" both of these objectives require an internet-hosted connection in order to be completed.[56] As a result, Internet-Hosted EHR technologies require more security policies and procedures to protect patients' PHI. Internet-Hosted EHR programs have potential security risks, such as, a vendor controlling the technologies' security settings, patient health information being stored outside of the United States, subjecting the information to different laws regarding the privacy and security of health information, and EPs/EHs relying on an unprotected internet connection to utilize EHR technology.[57] Additionally, EPs/EHs must consider the threat of a cyber-breach and implement cyber-security for their Internet-Hosted EHR technologies. Therefore, cyber-security is essential to the protection of PHI.[58] Even small and low profile EPs/EHs have to be concerned because "everyday there are new attacks aimed specifically at small to mid-size organizations because… they are less likely to have fully protected themselves."[59]

---

53. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 5.

54. *Id.* at 11.

55. *Id.* at 7.

56. *Eligible Professional Meaningful Use Table of Contents Core and Menu Set Objectives*, *supra* note 42.

57. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 20.

58. Cyber-security, "also referred to as information technology security, focuses on protecting computers, networks, programs[,] and data from unintended or unauthorized access, change[,] or destruction." *Cyber Security Primer*, UNIV. OF MD. UNIV. COLL., http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm (last visited Nov. 27, 2014).

59. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 13.

Furthermore, many cyber-attacks occur as a result of a failure to implement basic security measures beyond those which internally protect the EHR technology, such as requiring limited accessibility to a secure room where EHR technology is physically located, proper training of all individuals utilizing EHR technology, requiring individuals utilizing the technology to keep their access information confidential, and knowing when, where, and how often EHR technology is being backed up.[60] As a result of the lack of cyber-security measures, many EPs/EHs have fallen and will continue to fall victim to hacking.

ANALYSIS

As the healthcare profession continues to implement EHR technology into its everyday practices, it is inevitable that unless something is done to combat the large numbers of security and privacy breaches, such as hacking into patient's PHI, the numbers will continue to rise. For example, a survey conducted by Xerox in 2012 determined that nearly eighty-five percent of Americans believe that the security and privacy of their PHI will likely be disclosed as the result of continued adoption of EHR technology.[61] Additionally, in December 2012, the Ponemon Institute conducted a study regarding patient privacy and security, which "estimates the average price tag for dealing with breaches has increased from $2.1 million in 2010 to $2.4 million in 2012."[62] "The report projects that the economic impact of continuous breaches and medical identity theft could be as high as $7 billion annually, for the healthcare industry alone."[63] In 2013, "breaches in the healthcare/medical category surpassed all others, accounting for 43.1%, according to the Identity Theft Resource Center – more than business, government, financial/credit card or education."[64] In 2012, it was 34.9% of all breaches.[65] Moreover, in 2013, cyber-attacks within the healthcare industry had risen 40% from the 20% reported in 2009.[66]

---

60. *Id.* at 21.

61. Frank Quinn, *EHR and Security Concerns*, MEDCITYNEWS.COM (Sept. 26, 2012, 2:46 PM), http://medcitynews.com/2012/09/ehr-and-security-concerns/.

62. Alex Horan & Scott Rupp, *Healthcare Records: A Hacker's Roadmap to your Life*, ELECTRONIC HEALTH REPORTER (April 3, 2014), http://electronichealthreporter.com/healthcare-records-hackers-roadmap-life/.

63. *Id.*

64. Ken Donoghue, *How to Protect Health Data from Hackers*, PEAK 10 (Mar. 6, 2014), http://www.peak10.com/blog/post/how-to-protect-health-data-from-hackers#.VF6Oa74irzI.

65. *Id.*

66. *Your Medical Record is worth 10 times more to hackers than your credit card*, NY DAILY NEWS (Sept. 24, 2014, 4:27 PM), http://www.nydailynews.com/life-style/health/medical-record-worth-hackers-credit-card-article-1.1951536.

These increases can be attributed to the fact that EPs and EHs have low security procedures in place and as a result of the lack of adequate security, EPs/EHs open the door for hackers to obtain large quantities of PHI with relative ease.[67]

HACKING OF PHI

A patient's PHI can include a patient's name, address, birth date, telephone numbers, Social Security number, medical record number, health insurance number, and bio-metric identifiers, such as the patient's finger prints or full-face photographs of the patient taken by a medical provider.[68] Additionally, PHI includes, demographic information, information relating to the patient's physical and mental health[69] and "any other unique identifying number[s], characteristic[s] or code[s]."[70] A patient's PHI is analogized as being a roadmap of a person's life because once a person obtains this information they have access to a person's "social security numbers, insurance records, birth dates, family details, billing information, transactional history and…a detailed medical history."[71] As a result of a patient's PHI being such a comprehensive roadmap[72] of a person's life, it is not surprising that hacked PHI is so valuable on the black market.[73] Once a patient's PHI is in the hands of a hacker or unauthorized individual,[74] a single patient's information can be sold for approximately $10 to $50 on the black market.[75] As a result of the large monetary incentives, hackers/unauthorized individuals continue to hack into and sell patients' PHI.[76] Unfortunately, once a patient's PHI is in the hands of an unau-

---

67. *Id.*

68. *What is Protected Health Information (PHI)?*, INDIANA UNIVERSITY: KNOWLEDGE BASE, https://kb.iu.edu/d/ayyz (last visited Nov. 8, 2014).

69. *Protected Health Information*, HHS.GOV 3, http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/udmn.pdf (last visited Nov. 8, 2014).

70. *What is Protected Health Information (PHI)?*, *supra* note 68.

71. *Id.*

72. Horan, *supra* note 62.

73. *Id.*

74. Under the HIPAA Privacy Rule Authorization a patient must sign a permission "slip" giving a covered entity permission to "use or disclose the individual's protected health information (PHI) that is described in the Authorization for the purpose(s) and to the recipient(s) stated in the Authorization." *HIPAA Authorization for Research*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES NATIONAL INSTITUTES OF HEALTH, http://privacyruleandresearch.nih.gov/authorization.asp (last visited Nov. 8, 2014).

75. *Your Medical Record is worth 10 times more to hackers than your credit card*, *supra* note 66; Horan, *supra* note 62.

76. *Id.*

thorized individual, their PHI has become compromised and it is almost impossible to clear up.[77]

Unlike a credit card, a person cannot call and cancel their PHI and receive new information within a few business days. During a breach of an EP/EH's EHR technology, patients' PHI, billing, and insurance information will likely be stolen.[78] Under the HIPAA Breach Notification Rule EPs/EHs are required to notify individuals and the Secretary of U.S. Department of Health and Human Services (HHS) when there is a "loss, theft, or certain other impermissible uses or disclosures of unsecured protected health information."[79] In breaches that affect 500 or more individuals, the individuals and HHS must be promptly notified.[80] Additionally, when more than 500 residents of a state or jurisdiction have their PHI breached, the EP/EH must also notify the media.[81] However, when less than 500 individuals are affected, the breach can be reported to the HHS on an annual basis, and due "no later than 60 days after the end of the calendar year in which the breaches occurred."[82] Although these breaches are reported to the HHS the exact numbers of breaches are not made publically available.[83] Unfortunately, with regard to any breach, affecting a large or small number, a patient may discover their medical information has been stolen after someone has already used their PHI to impersonate them and receive their health benefits.[84] As a result, patients will often encounter large financial repercussions because someone stole their identity and PHI to receive care.[85] For example, "a Pennsylvania man found that an imposter had used his identity at five different hospitals in order to receive more than $100,000 in treatment."[86] "At each spot, the imposter left behind a medical history in his victim's name."[87] Sadly, that is just one example, since the creation of the HITECH Act in 2009 to 2013 there has been over 800 large breaches of protected health information (PHI) affecting over 29 million patient records.[88]

---

77. Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), http://kaiserhealthnews.org/news/rise-of-indentity-theft/.

78. Horan, *supra* note 62.

79. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 36.

80. *Id. at* 36.

81. *Id. at* 36.

82. *Id. at* 36.

83. *Breach Report 2013*, *supra* note 13.

84. Ollove, supra note 77.

85. *Id.*

86. *Id.*

87. *Id.*

88. *Breach Report 2013*, *supra* note 13.

As previously stated, one of the central goals for the shift away from paper medical records to electronic medical records, was to "improve quality, safety, and efficiency of patient health care."[89] However, as a result of hacking or breaching EP/EH's EHR technology, patients are at a great risk of being subjected to medical mistakes.[90] A study done by Ponemon Institute "revealed that the effect of medical identity theft can prove to be fatal."[91] Because another individual's medical information is being added to the victim's medical records, and as a result, an "incorrect blood type or prescription information could cause life-threatening complications at the point of treatment" and may ultimately lead to a patient's death.[92] Additionally, a patient's medical records can be "polluted" to the point where the patient is denied treatment or misdiagnosed based on the incorrect information being integrated into their PHI.[93] For example, a patient in Texas used a California man's medical identity to obtain radiation treatment and other care.[94] When the thief's records and the patient's were merged, healthcare providers thought the patient had a condition he did not.[95] A second example is, a teenager was denied the opportunity to be a blood donor after the Red Cross flagged her as HIV Positive.[96]

Additionally, patients that fall victim to PHI hacking must be concerned about their personal health history being disclosed to the public. Health information regarding a patient's mental health, substance abuse, HIV/AIDS status, as well as other diseases, carry a certain stigma within society and may lead to irrepressible "reputational harm."[97] This sensitive information can come up in an employment background check and other criminal and non-criminal settings.[98] Furthermore, a patient's medical record could be polluted by another individual's medical history and as a result that patient may be "wrongfully penalized based on information not even pertaining to them."[99] "In Oregon, a pregnant woman delivered a baby addicted to crack using another

89. *Welcome to the Medicare & Medicaid EHR Incentive Program Registration & Attestation System*, supra note 36.

90. Horan, *supra* note 62.

91. *Id.*

92. *Id.*

93. Christine Arevalo & Rick Kam, *A Glimpse Inside the $234 Billion World of Medical Fraud*, GOV. HEALTH IT (Feb. 8, 2012), http://www.govhealthit.com/news/glimpse-inside-234-billion-world-medical-id-theft.

94. *Id.*

95. *Id.*

96. *Id.*

97. Horan, *supra* note 62.

98. *Id.*

99. *Id.*

woman's social security number – and then abandoned the baby. Police arrested the victim and put her children into protective custody."[100]

In order for EPs/EHs to detect and prevent future hacking of their patients' PHI, EPs/EHs must first look to the security measures that are incorporated within their EHR technology.

SECURITY MEASURES EHR VENDORS MUST INCORPORATE INTO EHR TECHNOLOGY

In order for an EP/EH to achieve the meaningful use requirements of the EHR incentive program, EPs/EHs must first determine which EHR technology will best suit their business and their patients' needs. Under the Medicare and Medicaid incentive programs all EPs/EHs are required to use a certified electronic health record technology ("CEHRT").[101] This is because CEHRT gives EPs/EHs the "assurance…that an EHR system or module offers the necessary technological capability, functionality, and security to help them meet the MU [meaningful use] objectives and measures."[102] To become a CEHRT the EHR vendor must incorporate specific security requirements into its technology; these requirements are created and maintained by the Office of the National Coordinator for Health Information Technology ("ONC").[103] This is because under the HITECH Act the ONC was put in charge of creating and maintaining an EHR certification program and "[i]n 2010 the ONC established the ONC HIT Certification Program to oversee the certification and testing of EHR products."[104] Therefore, in order to be awarded certification from the ONC, EHR technology must include nine security requirements:

> (1) access control, [permitting] only authorized users to access electronic health information; (2) emergency access, [permitting] authorized users to access electronic health information during an emergency; (3) automatic log-off, [ending] an electronic session after a predetermined time of inactivity; (4) audit [logging], [recording] actions related to electronic health information; (5) [enabling] a user to generate an audit log for a specific time period and to sort entries; (6) integrity, [verifying] that electronic health information has not been altered in transmission and [detecting] the alteration of audit logs; (7) authentication, [verifying] that a person seeking access to electronic health information is the one claimed and is authorized to access the

100. *Id.*

101. *Certification Programs & Policy Certification and EHR Incentives*, HEALTHIT.GOV (on file with author).

102. *Id.*

103. *Id.*

104. *Id.*

> information; (8) encryption for general information; [and] (9) encryption when exchanging electronic health information.[105]

Although these are the only required security measures CEHRT must include, some EHR vendors have implemented additional security into their technology.[106] For example, an EHR vendor may include optional security measures such as, "accounting of disclosures… [recording] disclosures made for treatment, payment, and health care operations."[107] However, it is important for EPs/EHs to be aware that EHR vendors are not required to comply with any HIPAA Privacy and Security Rules in order to receive ONC certification.[108] Therefore, the burden of compliance falls solely on the EP/EH.[109] This is a heavy burden to put on EPs and EHs and as a result patients' PHI is being put unnecessarily at risk. Smaller healthcare providers in particular are unable to provide patients with adequate security measures because of both the technical difficulty and expense, which has led many providers to neglect e-PHI security and HIPAA compliance.[110]

SECURITY MEASURES EPS/EHS ARE IMPLEMENTING TO ACHIEVE MEANINGFUL USE

Once an EP/EH has chosen its EHR technology, the EP/EH has the burden of not only achieving the meaningful use requirements, but the EP/EH must also comply with all privacy and security measures included within the HIPAA Privacy and Security Rules.[111] This is because the "meaningful use requirements are not intended to supersede or substitute... compliance required under HIPAA."[112] For example, in order to comply with the HIPAA Security Rule, EPs/EHs are "required to implement policies and procedures to prevent, detect, contain, and correct

---

105. *How Do I Ensure Security in Our System?*, HRSA HEALTH INFORMATION TECHNOLOGY, http://www.hrsa.gov/healthit/toolbox/HIVAIDSCaretoolbox/SecurityAndPrivacyIssues/howdoiensuresec.html (last visited Nov. 8, 2014).

106. *Id.*

107. *Id.*

108. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 11.

109. *Id.* at 11.

110. Ben Watts, *Health IT Security and The Small Provider: A Primer for 2013*, EMRSOAP ADVANCING HEALTHCARE VIA SMARTER INFO. TECH. 3 (2013), http://www.emrsoap.com/wp-content/uploads/2012/12/Health-IT-Security-and-the-Small-Provider-A-Primer-for-2013.pdf.

111. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 7.

112. *Id.* at 7.

security violations."[113] To aid in achieving these policies and procedures EPs/EHs must conduct routine security risk checks.[114] The security risk analysis process requires EPs/EHs to consider multiple facets of their medical practices including, their "EHR software and hardware, [the] adequacy of … [their] practice protocols, [the] physical setting and environment, staff education and training, EHR access controls, contracts with … [their] business associates, [and] patient relations and communications."[115]

Once an EP/EH has taken into consideration the security risk analysis, HIPAA requires policies and procedures be written down, so that the EP/EH's staff knows "what is required and how to implement the policies and procedures."[116] As a guideline for EPs/EHs, the policies and procedures should include, what is required of the EP/EH and their staff, such as, requiring unique passwords and user names, "user and role based access controls [to] prevent inappropriate or unauthorized access to both patient information and system controls," encryption that protects PHI when records are transmitted and/or viewed from mobile devices, and installation of firewalls[117] and encryption[118] to maintain a secure network.[119]

Unfortunately, even after EPs/EHs have implemented additional security measures to comply with meaningful use as well as the HIPAA Privacy and Security Rules, hacking of patients' PHI continues to occur at increasing rates.[120] This increase is shown in the 2012 HHS report which determined that out of more than 200 healthcare security breaches, 53% involved theft of a physical device, like an EP/EHs' computer or mobile device, or the theft of a patient's paper record, while 9% of the security breaches were the result of patients' PHI being hacked into.[121] These results can be indicative of the healthcare provider's lack

---

113. *Id.* at 8.

114. *Id.* at 32.

115. *Id.* at 32.

116. *Id.* at 22.

117. A firewall is defined as "an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system." *Firewall*, DICTIONARY.COM, http://dictionary.reference.com/browse/firewall (last visited Nov. 27, 2014).

118. Encryption is defined as "the process of encoding a message so that it can be read only by the sender and the intended recipient." *Encryption*, DICTIONARY.COM, http://dictionary.reference.com/browse/encryption (last visited Nov. 27, 2014).

119. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 32.

120. Crissinda Ponder, *Are Your Electronic Health Records Safe?*, BANKRATE (Sept. 11, 2014), http://www.bankrate.com/finance/insurance/are-electronic-health-records-safe.aspx.

121. *Id.*

of effort to implement stricter security policies and procedures. A study conducted by BitSight Technology indicates that healthcare providers are "spending less on IT security than other businesses."[122] A survey conducted by the "Healthcare Information and Management Systems Society, with support from the Medical Group Management Association," concluded that 49% of "survey respondents… reported spending 3[%] or less of their overall IT budgets on it [security], which is less than adequate, according to industry experts."[123] Additionally, 19% of the survey "respondents reported their organizations had experienced a security breach and 12[%] had a known incident of medical identity theft."[124]

Therefore, the security measures that EPs/EHs are implementing to achieve meaningful use and comply with the HIPAA Privacy and Security Rules have been shown to be "less than adequate"[125] and something must be done to improve PHI security.

CONSEQUENCES OF NON-COMPLIANCE WITH HIPAA PRIVACY AND SECURITY RULES

In order to force EPs/EHs to comply with HIPAA Privacy and Security Rules, HIPAA can impose civil and criminal penalties.[126] If an EP/EH fails to appropriately secure its patient's information the Office of Civil Rights (OCR) is responsible for "administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules… investigations, compliance reviews, and audits."[127] Violation penalties are based on "the nature and extent of the violation and the nature and extent of the harm resulting from violation."[128]

---

122. *Hacking is bad for your health*, THE TENNESSEAN (Aug. 23, 2014), http://www.tennessean.com/story/opinion/editorials/2014/08/23/hacking-bad-health/14499887/ (last visited Nov. 8, 2014). *See also* Robert Lemos, *CHS Breach a Sign of Health Care's Security Illness*, EWEEK.COM (Aug. 24, 2014), http://www.eweek.com/security/chs-breach-a-sign-of-health-cares-security-illness.html.

123. Joseph Conn, *Healthcare Providers Boost Security Spending: HIMSS Survey*, MODERN HEALTHCARE (Feb. 20, 2014), http://www.modernhealthcare.com/article/20140220/NEWS/302209951. *See also Retailers spend less on cybersecurity than other industries, and it shows*, HOMELAND SECURITY NEWS WIRE (Sept. 5, 2014), http://www.homelandsecuritynewswire.com/dr20140905-retailers-spend-less-on-cybersecurity-than-other-industries-and-it-shows.

124. Conn, *supra* note 123.

125. *Id.*

126. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 37.

127. *Id.* at 37.

128. *HIPAA Violations and Enforcement*, AMERICAN MEDICAL ASSOCIATION, http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-

Civil penalties for failure to comply include instances in which:

> Individual[s] did not know … that he/she violated HIPAA, [there was a] HIPAA violation due to reasonable cause and not due to willful neglect, [there was a] HIPAA violation due to willful neglect but [the] violation is corrected within the required time period [30 days, however, this period may be extended], and [there was a] HIPAA violation [that was] … due to willful neglect and is not corrected.[129]

These violations have ranging fines from a minimum of $100 per violation to an annual maximum of $1.5 million.[130]

Furthermore, criminal penalties can be imposed against an EP/EH that has, "knowingly [obtained] or [disclosed] individually identifiable health information in violation of the Administrative Simplification Regulations, and these EPs/EHs face fines up to $50,000, as well as imprisonment up to one year."[131] Also:

> Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison [and] … offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permits fines of $250,000, and imprisonment for up to ten years.[132]

Additionally, the HITECH Act "increases noncompliance penalties and incentives for covered entities to implement an EHR."[133] HITECH also further "extends requirements of the HIPAA Security Rule and some aspects of the HIPAA Privacy Rule to business associates."[134]

For example the HHS OCR began an investigation into Idaho State University's ("ISU") Pocatello Family Medicine Clinic, when it notified HHS that 17,500 of its patients' e-PHI was unprotected for over 10 months as a result of disabled firewall servers maintained by ISU.[135]

---

practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page? (last visited Nov. 8, 2014).

129. *Id.*

130. *Id.*

131. *Id.* The Administrative Simplification Regulations are provisions within HIPAA which requires HHS to "adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security." *HIPPA Administrative Simplification Statute and Rules*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/ (last visited Nov. 8, 2014).

132. *HIPAA Violations and Enforcement*, *supra* note 128.

133. *Who Must be HIPAA Complaint?*, SECUIRTYMETRICS, https://www.securitymetrics.com/hipaa-overview (last visited Nov. 9, 2014).

134. *Id.*

135. *Idaho State University Settles HIPAA Security Case for $400,000*, U.S. DEPT. OF HEALTH & HUMAN SERV. (May 21, 2013),

Following the investigation, the OCR found that ISU's "risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities."[136] As a result, ISU agreed to pay $400,000 to HHS to settle the "alleged violations" of the HIPAA Security Rule.[137]

Unfortunately, even with these fines and penalties in place, medical providers continue to lack adequate security measures that will lead to the reduction of hacking and breaching PHI.[138]

PROPOSAL

In order to combat the steady increase of EHR technology being breached, certain modifications to the EHR incentive program and HIPAA Privacy and Security Rules need to be made. To make a meaningful impact on the way EHR technology is being implemented and utilized EHR vendors will have to incorporate additional security measures into their technology, EHR vendor's trainers will have to become adequately informed about compliance with HIPAA security standards, and EPs/EHs will have to become better educated about implementing adequate security policies and procedures.

EHR Technology Must Include HIPAA Compliant Security Measures

First and foremost EHR vendors should be required to comply with HIPAA standards in order to obtain ONC certification. To that end, EHR technology must incorporate specific security measures that expand upon the ONC's nine security requirements that are currently in place.[139] At this time, EHR vendors are not required to create technolo-

---

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement-press-release.html.html.

136. *Id.*

137. *Id.*

138. *Hacking is bad for your health*, *supra* note 122.

139. *How Do I Ensure Security in Our System?*, *supra* note 105; The nine security requirements that all EHR technology must include are:

> (1) access control, [permitting] only authorized users to access electronic health information; (2) emergency access, [permitting] authorized users to access electronic health information during an emergency; (3) automatic log-off, [ending] an electronic session after a predetermined time of inactivity; (4) audit [logging], [recording] actions related to electronic health information; (5) [enabling] a user to generate an audit log for a specific time period and to sort entries; (6) integrity, [verifying] that electronic health information has not been altered in transmission and [detecting] the alteration of audit logs; (7) authentication, [verifying] that a person seeking access to electronic health information is the one claimed and is authorized to access the information; (8) encryption for general information; [and] (9) encryption when exchanging electronic health information.

gy that is compliant with any HIPAA Privacy and Security Rules.[140] As a result, EPs/EHs are solely responsible for creating policies and procedures that will achieve the goals of the HIPAA Privacy and Security Rules.[141] Unfortunately, the reality of the situation is, that healthcare providers are not only spending less on IT security than other businesses[142] but they are in a worse position to implement the technological solutions. Therefore, the best way to combat this problem is to require the EHR vendors to incorporate additional HIPAA compliant standards into their technology.

These additional standards should include, stricter password protections, the ability to redact information including sensitive information prior to transmittal of patients' PHI, additional encryption procedures for patients with sensitive medical information, the ability to segregate portions of patients' PHI containing sensitive information, and the ability to block access to specific areas of patients' PHI. By requiring the incorporation of these additional security measures into the EHR technology, the technology will become harder to hack into, therefore, making the technology more secure against hackers and unauthorized individuals.

In order to maintain the protection of patients' PHI, EHR vendors should be required to implement additional password protection standards. These password protection standards should include requiring passwords to contain specific characters, for example, at least one capital letter, at least one number, at least one non-alphanumeric symbol, as well as a password length requirement. EHR technology that is created to cater to EPs/EHs dealing with sensitive information, such as mental health, substance abuse, and HIV/AIDS patients, should be required to incorporate a higher level of security access, such as a password and bio-metric scan (i.e. finger print or retina scan).[143] Moreover, the EHR software should require users to change their password at regular intervals and prevent system access after several failed login attempts.[144] Even with these password protections incorporated within the EHR software, EPs/EHs still have the burden to inform their staff about the importance of maintaining the security of their passwords.[145]

Id.

140. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 11.

141. *Id.*

142. *Hacking is bad for your health*, *supra* note 122.

143. *Protecting Patient Data: Procedures and Practices to Maintain Data Security*, NYC.GOV, http://www.nyc.gov/html/doh/downloads/pdf/csi/ehrkit-protect.pdf (last visited Nov. 8, 2014).

144. *Id.*

145. *How Do I Ensure Security in Our System?*, *supra* note 105.

Therefore, although incorporation of these security protections within the EHR software makes it easier for an EP/EH to comply with HIPAA the burden of compliance still falls on the EP/EH.

Additionally, EHR technology should be required to include the ability to redact, encrypt, and segregate sensitive information.[146] These functions have been implemented in the technology of other industries and have been proven to be an effective way to protect information. "Many financial companies have used encryption for years and they probably wonder what the heck is going on with the health care industry … it's much cheaper to deploy safeguards than to suffer a breach."[147] Furthermore, these functions would be required in order to maintain the integrity of a patient's sensitive PHI.[148] This is because, "the law affords special protection to certain diagnoses or conditions."[149] Within the healthcare community, mental health, substance abuse, and HIV/AIDS patients must be afforded a higher level of confidentiality and these patients must have their privacy protected, "to ensure they have the same considerations as others in the community and that they do not fall prey to identity theft or fraud."[150]

With regard to HIV/AIDS, a patient's EP/EH is required to report these conditions, and therefore in order to maintain the security of this information the EHR technology must include the ability to encrypt it so that the patient's sensitive PHI is not accessible to unauthorized individuals.[151] To do this "EHR systems must provide mechanisms that enable facilities to manage the extra layer of protection for this information … particularly for release of information purposes."[152]

EHR technology should also be required to include the ability to segregate sensitive information. "Organizations must have the ability to segregate any records related to treatment of substance abuse and chemical dependency, as treatment of these patients can encompass

---

146. AHIMA e-HIM Work Group on Security of Personal Health Information, *Ensuring Security of High-Risk Information in EHRs*, JOURNAL OF AHIMA 79, no.9 67-71 (Sept. 2008), http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039956.hcsp?dDocName=bok1_039956.

147. David Schultz, *As Patients' Records Go Digital, Theft and Hacking Problems Grow*, KAISER HEALTH NEWS (June 3, 2012), http://kaiserhealthnews.org/news/electronic-health-records-theft-hacking/ (*Quoting* Deven McGraw, Direct of the Health Privacy Project at the Center for Democracy and Technology).

148. AHIMA e-HIM Work Group on Security of Personal Health Information, *supra* note 146.

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

multiple medical specialties and document types."[153]

Finally, EHR technology should be required to incorporate the ability to block access to specific areas of patients' PHI depending on who is attempting to access the information and for what purpose. This can be done by "[restricting] patient[']s [records] from physicians who are not the 'physician of record' (e.g. attending, admitting, surgical, and consulting physician), [the] ability to block access to a specific progress note or lab result, [and the] ability to track versioning or mask sensitive entries for release of information."[154]

By requiring EHR vendors to incorporate these security standards into their technology to receive ONC certification EPs/EHs can be assured that not only will the EHR technology meet the meaningful use requirements, but the technology will also provide assurance of its compliance with the HIPAA Privacy and Security Rules. As a result of shifting the burden of implementation of these standards to the EHR vendors, patients' PHI is more likely to be adequately secured.

Trainers Must Obtain HIPAA Certification

Beyond requiring EHR technology to comply with HIPAA Privacy and Security Rules, having the appropriate knowledge of the law is essential to improve the quality of patient security with regard to PHI. In order to achieve this goal I propose the creation of a certification process that all EHR trainers must obtain prior to being permitted to train EPs/EHs on how to use its EHR technology.

This certification process should require EHR trainers to participate in a three-step certification process, similar to that which insurance agents are required to go through to become licensed to sell insurance.[155] Insurance agents must obtain a license to be able to participate in the "solicitation, selling, or negotiation of insurance."[156] In order to receive an insurance license, individuals are required to complete course work, pass several examinations, and obtain a license within the state(s) they wish to work.[157] The requirements for most states' insurance agent certification programs include enrollment in a school which provides: "(1) 20-40 or more hours of General Insurance courses; (2) 6-

153. *Id.*

154. AHIMA e-HIM Work Group on Security of Personal Health Information, *supra* note 146.

155. How to Get an Insurance or Securities License, INSURANCELICENSEEXPRESS.COM, http://www.insurancelicenseexpress.com/general/how-to-get-insurance-license.asp (last visited Nov. 8, 2014).

156. *Id.*

157. *Id.*; Specific requirements vary by state. *Id.*

12 hours of Ethics courses; and (3) practice exams and quizzes."[158] Upon the completion of the required course work, states require individuals to pass a licensing exam, which tests the individual's knowledge of general and state specific insurance laws.[159] Additionally, once an individual becomes licensed, they must participate in mandatory continuing education programs in order to maintain their license.[160] In most states, the "mandatory continuing education requirements focus[e] on insurance laws, consumer protection, ethics, and the technical details of various insurance policies."[161]

Another influence for this certification program comes from the Certified HIPAA Professional (CHP) program.[162] This program is a two-day instructor led program that focuses on the Administrative Simplification portion of HIPAA as well as examining the "HIPPA Transactions and Code Sets, Identifiers, Privacy and Security."[163] During this training individuals learn how to "create a framework for initiating and working towards a blueprint for HIPAA compliance."[164] Participation within this program provides individuals with knowledge of:

> (1) understanding why HIPAA requirements will cause significant changes in policies, procedures[,] and processes within the organization in the handling of patient records; (2) [examining] how implementing HIPAA will affect the way healthcare entities organize and staff to achieve and monitor compliance with patient privacy/confidentiality needs; (3) … qualifications and positioning strategies for a Chief Privacy Officer and requirements for a Chief Security Officer; (4) [learning] why HIPAA compliance is better focused as a business issue than as an IT issue, although IT will play a major role in implementing complaint systems; and (5) review specific requirements and implementation features within each security category.[165]

Following the completion of this course individuals are required to take the CHP examination in which the largest portion of this exam focuses on HIPAA Security.[166] The CHP examination is a total of 60 questions in 60 minutes, focusing on "HIPAA Administrative Simplification Over-

---

158. *Id.*

159. *Id.*

160. How to Get an Insurance or Securities License, *supra* note 155.

161. *Id.*

162. Certified HIPAA Professional (CHP), HIPPA ACADEMY, http://www.hipaaacademy.net/credential-offerings/certified-hipaa-professional-chp/ (last visited Nov. 8, 2014).

163. *Id.*

164. *Id.*

165. *Id.*

166. CHP Exam, ECFIRST ONLINE STORE, http://www.hipaacertificationonline.com/CHP.html (last visited Nov. 8, 2014).

view (28%), HIPAA Privacy (22%), HIPAA Transactions and Code Sets (20%), and HIPAA Security (30%)."[167]

In order to effectively create a program that will provide EHR trainers with adequate knowledge of the HIPAA Privacy and Security Rules I propose the creation of a program that is a combination of the insurance licensing program and the CHP program. As previously stated, this will work as a three-step process: (1) expert level; (2) knowledge level; and (3) awareness level.

Within the expert level of the program participants would be required to complete course work and quizzes similar to that which occurs in the insurance licensing program. These courses and quizzes would focus primarily on the HIPAA Privacy and Security Rules and effective means to comply with these rules. Following the completion of the required course work, individuals would be required to take a state certification examination. The state certification examination would test an individual's ability to adequately understand the HIPAA Privacy and Security Rules as well as test their ability to implement strategies and procedures that combat non-compliance with HIPAA, such as hacking and other breaches of patients' PHI.

The knowledge level of this certification program would consist of a bi-annual re-certification examination. As technology becomes more integrated into the healthcare industry EHR technology vendors as well as medical care providers must continue to adapt to possible breaches in security.[168] In order to do so EHR trainers and EPs/EHs need to be educated on how to properly deal with new situations.

The third and final stage, the awareness level, of the EHR trainer certification program would be similar to the insurance licensing continuing education programs. Within the insurance industry the number of required continuing education hours per period depends on your license type as well as the state in which you are licensed.[169] In Texas, for example, a general insurance agent that is licensed to sell life, accident, health, and HMO insurance is required to complete 30 hours of continuing education within a two-year period, including "2 hours of ethics/consumer protection."[170] Therefore, during this stage of the certification process trainers would be required to complete a certain number of credit hours per year in order to maintain their certification.

---

167. *Id.*

168. *Healthcare Data Breaches on the Rise as New Technology is Introduced*, TREND MIRCO BLOG (Dec. 6, 2011), http://blog.trendmicro.com/healthcare-data-breaches-on-the-rise-as-new-technology-is-introduced/.

169. *See Continuing Education Information for Agents and Adjusters*, TEXAS DEPARTMENT OF INSURANCE, http://www.tdi.texas.gov/licensing/agent/agcehome.html (last visited Nov. 8, 2014).

170. *Id.*

Continuing education hours can be completed by attending or participating in HIPAA Privacy and Security Rule seminars and presentations.[171]

Overall the main goal of the EHR trainer certification program is to provide EHR trainers with the knowledge and skills required to aid EPs/EHs to effectively utilize their EHR technology in compliance with HIPAA Privacy and Security Rules.

Continuing Education for EPs/EHs Regarding Security

Medical professionals "have a legal, moral, and ethical duty to protect all clinical and research information by ensuring that security and privacy safeguards are in place."[172] In order for medical professionals to have the ability to comply with their legal, moral, and ethical duties, they must first be adequately educated. Therefore, one of the most influential ways to combat EHR privacy and security issues, such as hacking, will be to provide the medical professionals that utilize the technology with adequate knowledge of how to secure patients' PHI and how to maintain and update security measures in ways that will prevent future breaches. In order to achieve this goal I suggest EPs/EHs be required to complete a fixed number of hours of continuing education courses focusing primarily on HIPAA security. As of 2013, medical professionals in Illinois were required to complete 150 hours of continuing education over the course of three years.[173] However, continuing education credit hours per year vary by State.[174] Instead of requiring medical professionals to complete additional hours, one alternative is for medical professionals to complete 5 hours per year, or 15 hours over the course of three years that focus solely on HIPAA security. Because continuing education credit hours vary per state, my proposed number of credit hours focusing on HIPAA Security can be altered to best suit the specific state requirements while still maintaining the overall goal of providing medical professionals with adequate knowledge to improve patient security. Upon completion of these continuing education courses medical professionals would have the knowledge required to implement security and privacy measures that should effectively combat new security issues.

---

171. *Id.*

172. AHIMA e-HIM Work Group on Security of Personal Health Information, *supra* note 146.

173. *Continuing Medical Education for Licensure Reregistration*, DUKE UNIVERSITY, http://www.audio-digest.org/CME-State-CME-Requirements (last visited Nov. 8, 2014).

174. *Id.*

CONCLUSION

In the age of technology, it is not surprising that the healthcare industry has finally began to utilize technological advances to "improve the quality, safety, and efficiency of patient health care."[175] However, the healthcare industry has yet to master the "art" of protecting patients' PHI. The 2014 Community Health System breach is a prime example that something beyond the current requirements must be put into place.[176] Unfortunately, as a result of EPs/EHs spending less on IT security,[177] and failing to implement basic security measures patients' PHI can be easily hacked.[178]

In order to adequately protect patients' PHI, amendments to the ONC EHR certification requirements must be made. Currently EHR vendors are not required to comply with the HIPAA Privacy and Security Rules, leaving security policies and procedures solely in the hands of the EPs/EHs.[179] With my proposed changes to the ONC certification process, EHR vendors would be required to include within their technology, stricter password protections, the ability to redact information, the ability to segregate portions of patients' PHI, and the ability to block access to specific areas of patients' PHI. These additional security measures would give EPs/EHs the assurance that their EHR technology is not only capable of achieving the meaningful use requirements, but also is complaint with the HIPAA Privacy and Security Rules.

Beyond creating EHR technology that complies with HIPAA Privacy and Security Rules I believe educating the EHR vendor's trainers will be beneficial and improve overall security. Because EHR trainers are on the "front lines" while the technology is being tested and implemented these individuals are a great resource for information about how to effectively use the technology and combat possible security breaches. These individuals can provide medical professionals with sample policies and procedures that not only comply with HIPAA Privacy and Security Rules, but also work best with the specific technology being used.

While stricter requirements for ONC certification and requiring EHR trainers to become HIPAA certified will likely reduce hacking and security breaches, medical professionals still remain the individuals

---

175. *Welcome to the Medicare & Medicaid EHR Incentive Program Registration & Attestation System*, CENTERS FOR MEDICARE & MEDICAID SERV, https://ehrincentives.cms.gov/hitech/loginCredentials.action (last visited Nov. 8, 2014).

176. Perlroth, *supra* note 1.

177. *Hacking is bad for your health*, *supra* note 122.

178. THE OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH. *supra* note 10, at 11.

179. *Id.* at 11.

who "have a legal, moral, and ethical duty to …ensure that security and privacy safeguards are in place."[180] Therefore, medical professionals should be required to complete continuing education courses specifically focusing on HIPAA security issues. These courses would be beneficial because they would allow medical professionals the opportunity to gain an understanding of new security threats and how to combat these threats, and as a result medical professionals will use this knowledge to implement improved policies and procedures to protect their patients' PHI.

Therefore, I strongly believe that by requiring EHR technology vendors to incorporate specific HIPAA complaint standards within their technology, requiring EHR technology trainers to obtain HIPAA certification, and requiring medical professionals to complete a minimum number of continuing education credits focusing on HIPAA security the number of PHI breaches will begin to decline.

180. AHIMA e-HIM Work Group on Security of Personal Health Information, *supra* note 146.