Minnesota Journal of Law, Science & Technology

Volume 20 | Issue 1 Article 13

8-7-2019

Bleeding Out: The Case for Strengthening Healthcare Client Portal Data Privacy Regulations

Matthew D. McCord

Note

Bleeding Out: The Case for Strengthening Healthcare Client Portal Data Privacy Regulations

Matthew D. McCord[*]

On a cool, May Friday in Long Beach, California, one of the largest managed healthcare companies in the United States abruptly yanked its patient portal system out of production.[1] Molina Healthcare ("Molina") pulled its key customer-facing system because of a dangerous set of application security faults lurking in the code after a security researcher reported an anonymous tip.[2] The application reportedly failed to authenticate patients against their claims and passed claim IDs through plain, user-modifiable URL text, allowing any user to view any other claim just by changing the URL.[3] The data compromised included individualized, valuable, and closely-guarded protected health information (PHI), including patient names, addresses, dates of birth, diagnoses, and prescriptions among other data points and descriptors, opening patients to damaging leaks of their private health and to medical fraud.[4]

[*] JD Candidate 2019, University of Minnesota Law School.

[1] Jessica Davis, *Molina Healthcare Breached, Exposed Patient Data for Over a Month*, HEALTHCARE IT NEWS (May 30, 2017), http://www.healthcareit-news.com/news/molina-healthcare-breached-exposed-patient-data-over-month (describing the security breach that occurred at Molina Healthcare, a company that provides health care services to low-income families and individuals). For information on Molina's size and headquarters location, see *Molina Healthcare*, FORTUNE 500, http://fortune.com/fortune500/molina-healthcare/ (last visited Dec. 3, 2017). For information on local weather on the date of the incident response, see *Weather History for Long Beach, CA*, WEATHER UNDERGROUND, https://www.wunderground.com/history/airport/KLGB/2017/5/26/DailyHistory.html?req_city=&req_state=&req_statename=&reqdb.zip=&reqdb.magic=&reqdb.wmo= (last visited Dec. 3, 2017).

[2] Davis, *supra* note 1.

[3] *Id.*

[4] *Id.*

Yet, the data contained in insurer portals can pale in comparison to the extensive data held by and across particular healthcare providers (e.g. one's primary doctor or cardiologist).[5] While insurer data may include generalized data about claims, provider portals can contain compendiums of full lab results, summaries of care, patient concerns, practitioner impressions, personal and relatives' contact information, and billing data.[6] While Molina quickly stated that it was in the "process of conducting an internal investigation to determine the impact" of the breach, and that "protecting [its] members' information is of utmost importance[,]" the researcher behind the revelation, Brian Krebs, remained unnerved.[7] Mr. Krebs stated that it was "unconscionable that such a basic, Security 101 flaw could still exist at a major healthcare provider today," yet notes that these "serious vulnerabilities" are far from disparate events, but are rather common and pressing problems in the United States' national health and cybersecurity infrastructure.[8]

[5] *See What is a Patient Portal?*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/faqs/what-patient-portal (last visited Dec. 3, 2017) (finding that the most comprehensive portals have virtualized office visits, secure provider-to-patient messaging, benefits and coverage information, financial and billing information, relatives' medical summaries, and comprehensive medical histories stored on or, at a minimum, processed through their servers); *see, e.g.*, *Blue Cross Online Visits*, BLUE CROSS BLUE SHIELD OF MICH., https://www.bcbsm.com/index/find-a-doctor/online-visits.html (last visited Mar. 8, 2018).

[6] *See What is a Patient Portal?*, *supra* note 5 (concluding that billing data includes financially sensitive data like credit card numbers, insurance group and member numbers, prescription billing information, bank account numbers, and other information used to pay and validate payment between patients, providers, and payers).

[7] Davis, *supra* note 1.

[8] *See id.* The flaw itself was exposure of a "GET" request, reflecting this "basic, Security 101" error that was "unconscionable" in its existence. This reflection, by industry standards, sounds largely in truth and common sense. *See, e.g.*, Kevin Beaver, *Why Use POST vs. GET to Keep Applications Secure*, TECHTARGET (Feb. 2010), http://searchsoftwarequality.techtarget.com/tip/Why-use-POST-vs-GET-to-keep-applications-secure (finding that businesses should avoid using GET requests at all costs); Paris Mitton, *Never Put Secrets in URLs and Query Parameters*, FULLCONTACT (Apr. 2016), https://www.fullcontact.com/blog/never-put-secrets-urls-query-parameters/ (finding that URLs and query parameters aren't secure). Indeed, the data-passing flaw and subsequent failure-to-authenticate flaw are both listed in the Open Web Application Security Project's database as common vulnerabilities, with the authentication failure cited as one of the ten most critical application security risks. OPEN WEB APPLICATION SEC. PROJECT, *OWASP TOP 10 – 2017*:

Cybersecurity has loudly slammed the world of healthcare in recent years, with the severity and frequency of attacks on the national healthcare infrastructure attracting the noticeable scrutiny of the federal government.[9] Healthcare has become a substantially attractive cyberattack vector with the advent of the Internet of Things and its spread into life-critical systems like insulin pumps, increased device interconnectedness, rapidly spreading digitization, and increasing public demand for and activation of open access vectors for patients to view their information.[10]

The Ten Most Critical Web Application Security Risk , 12 (2017), https://www.owasp.org/index.php/Top_10-2017_Top_10 (denoting as a critical application vulnerability the uncontrolled, i.e. unchecked, access to sensitive web application data layers and systems through improper validation and control of POST requests, the alternative, more secure, web application request type to GET, as occurred in this particular case); *Data Validation*, OPEN WEB SEC. APPLICATION PROJECT, https://www.owasp.org/index.php/Data_Validation (last modified Dec. 1, 2013) ("strongly discourag[ing] . . . GET request" protocols for sending data except for navigational purposes). Yet, these vulnerabilities are seen, despite clear industry standards being set, repeatedly in notes on vulnerabilities in all manner of applications. *See, e.g.*, *CVE-2017-6086*, NAT'L VULNERABILITY DATABASE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6086 (last visited Mar. 8, 2018); *NVD - CVE-2017-12212*, NAT'L INST. OF STANDARDS AND TECH., https://nvd.nist.gov/vuln/detail/CVE-2017-12212 (last visited Mar. 8, 2018).

[9] HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY 5 (June 2017) (discussing and developing recommendations on the growing challenge of cyber attacks targeting health care).

[10] *Id.* at 10. For a discussion of the extensive cybersecurity concerns with medical devices, *see generally* John G. Browning & Shawn Tuma, *If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices*, 67 S.C. L. REV. 637 (2016) (finding that there is panic over hackable pacemakers, for example, which reflects cybersecurity concerns grounded in realism, with unconscionable consequences of failures and shortcomings). As patient portals often store medical records of patients, including their prescription records, care summaries, and present conditions, data on which medical professionals rely in making treatment decisions, a carefully-constructed attack on a patient record system could foreseeably lead to similarly austere harms as those posited by RFID pacemakers and similar medical devices. *See What is a Patient Portal?*, *supra* note 5 (describing the kinds of records that can be processed and contained on patient portals); Shahid Mansuri, *How Patient Portals are Improving the Virtual Healthcare System*, VALIDIC (Jan. 4, 2018), https://validic.com/how-patient-portals-are-improving-the-virtual-healthcare-system/ (discussing and analyzing how the adoption of patient portals have integrated this particular bit of technology with the active medical practices and decisions of a broad swathe of medical professionals, especially in on-demand care, as the march toward medical efficiency continues); *Patient Portal Benefits Patient Care and Provider Workflow*,

This Note seeks to examine the field of cybersecurity as it intersects with healthcare through an examination of the security of provider and insurer portals and the data contained on them, describe the security concerns flowing out of health information digitization, and provide for remediation of these concerns in an increasingly digital and increasingly digitally-besieged world. Part I will cover relevant background information on patient portals generally, the scope and value of health records stored on these portals, the rapidly-increasing vectors for digital attacks on national healthcare infrastructure, the evolution of distributed application security generally, the statutory schemes for regulating health portal data, and findings of liability for health data breaches. Part II will explore the ways in which proper healthcare portal data security furthers the national interest and the adequacy of the current and proposed statutory scheme's coverage of portal data. Part III will describe ways to create proper healthcare data security across the industry through a proposed legislative framework to address the continually-evolving challenges of healthcare IT. The Note will then conclude by stating that the hazards of insecurity discussed threaten national security, and the technology surrounding health data portals should reflect that risk through a comprehensive and enforceable but flexible statutory framework designed to supersede the present piecemeal approach to data security in the sector.

I. BACKGROUND

This background section will introduce the relevant historical background and recent developments pertaining to patient healthcare portals, including insurance claim and customer databases and provider servicing applications. This part will include a discussion of breaches at health providers and health insurers inclusive of physical plant breaches. This part will also discuss the vast increase in vectors for obtaining healthcare information and thus vectors for attack, with particular focus on web portals and the rise of state actors and

HEALTHIT.GOV, https://www.healthit.gov/case-study/patient-portal-benefits-patient-care-and-provider-workflow (last reviewed Sept. 19, 2017) (describing a government industry information release using the case study of a Primary Health Medical Group in Idaho to relay a similar message as Mr. Mansuri in relation to the benefits and contingent reliance of medical professionals on patient portals).

powerful, well-resourced groups hijacking information in recent years. This discussion ends by introducing the hodgepodge regulatory and statutory framework for healthcare data protection and the bases for liability to which healthcare businesses may expose themselves due to inadequate data protection policies.

A. History of Patient Portals

A patient portal, per the U.S. government, is "a secure online website that gives patients convenient[,] 24-hour access to personal health information from anywhere[.]"[11] Online medical portals entered rapid adoption in 2011 as part of the Meaningful Use technology investment program incorporated in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.[12] The HITECH Act allocated $19.2 billion to fund health information technology development, with expenditures guided by the Meaningful Use program requirements.[13]

Specifically, the Meaningful Use requirements provided a carrot-and-stick approach to enforcing adoption among Medicare and Medicaid servicing providers.[14] With HITECH foreseeing a problem of then-low health information technology provider adoption rates due to the high implementation costs of these

[11] *See What is a Patient Portal?*, *supra* note 5. As briefly discussed in that note and accompanying sources, health portals can range from a "barebones" summary of care received or appointment scheduling interface to a one-stop, unified records, access, care, and financial system spanning entire amalgamated care and hospital networks as these systems deign to provide maximal efficiency and unified user experience/single location benefits for providers, patients, and payers; *see also* Mansuri, *supra* note 10 (explaining the developments made in patient portal technology).

[12] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001, 123 Stat. 115, 231 (Feb. 17, 2009) (containing HITECH after consolidation of the bills in question); Terese Otte-Trojel et al., *Characteristics of Patient Portals Developed in the Context of Health Information Exchanges: Early Policy Effects of Incentives in the Meaningful Use Program in the United States*, J. MED. INTERNET RES., Nov. 21, 2014, at e258-1, 2 (finding that HITECH included USD 30 billion for accelerating and mainstreaming the use of health information technology).

[13] CHRISTINE PETERSON, HEALTH INFORMATION EXCHANGES AND PATIENT PORTALS IN BEHAVIORAL HEALTH 7 (2015).

[14] *See* Nicolas P. Terry, *Certification and Meaningful Use: Reframing Adoption of Electronic Health Records as a Quality Imperative*, 8 IND. HEALTH L. REV. 43, 50 (2011) (finding that Medicaid and Medicare incentive payments will be made to doctors).

systems, the Act provided subsidies for implementation of substantial electronic health record (EHR) systems, which include the functionality offered by patient portals as integrated EHR systems.[15] The incentive program ran its five-year course in 2016, and the incentives became penalties to participating providers, with hospitals failing to use EHR systems for "meaningful purposes" docked one to five percent per year of their Medicare and Medicaid reimbursement payments.[16]

This spring of grant finances, the threat of Medicare penalties, and the business logic in moving toward online storage of patient information rapidly shifted many providers away from paper-centric information management and toward digital record solutions.[17] Adopting patient portals can provide for the more efficient practice of medicine and can enhance the quality of care patients receive, enabling remote interactions to better use physician and patient time if adopted properly.[18] In

[15] *See* 42 C.F.R. § 495.102(b) (Oct. 1, 2017) (containing detailed provisions regarding incentive amounts); *see also* Terry, *supra* note 14 (finding that a physician participating in the full five-year incentive program "could receive the maximum subsidy of $44,000 through Medicare" if not employed through their hospital; hospital systems are eligible for a $2 million baseline, with additional monies disbursed based on a formula regarding inpatient discharges).

[16] *See* 42 C.F.R. § 495.102(d) (Oct. 1, 2017); Terry, *supra* note 14 (discussing that starting in 2016, HITECH's "carrots" will be replaced by "sticks"); AM. HEALTH LAWYERS ASS'N, *Meaningful Use Adjustments*, 2 HEALTH L. PRAC. GUIDE § 25:37 (2017) ("Beginning in 2015, CMS will negatively adjust the reimbursement of physicians and certain other eligible professionals who do not meet the 'meaningful use' criteria related to their use of EHRs.").

[17] *See* Kristine Crane, *How Patient Portals are Changing Health Care*, U.S. NEWS AND WORLD REPORT (June 30, 2014), https://health.usnews.com/health-news/patient-advice/articles/2014/06/30/how-patient-portals-are-changing-health-care (discussing the general shift of medicine to online service delivery and its consumer use case, namely doing away with physically-encumbering paper files and providing for speed and ease of communication between patient-consumer and physician, as well as single-practice numbers in a portal-implementing provider setting indicating an adoption rate of roughly three-quarters). Patient portals have been heavily advocated in the business context of healthcare service delivery due to consumer demand and efficiency pressures. *See, e.g.*, Heather Landi, *The Business Case for Increasing Patient Portal Adoption*, HEALTHCARE INFORMATICS (Jan. 7, 2016), https://www.healthcare-informatics.com/article/business-case-increasing-patient-portal-adoption; Elizabeth W. Woodcock, *How Patient Portals Create Value for Patients—and Fulfill Meaningful Use Requirements*, http://www.medfusion.net/docs/Patient%20Portals%20MU%20white%20paper.pdf. (retrieved Dec. 1, 2017).

[18] *See generally* Daniel F. Shay, *A Window Into Patient Portals: Legal and Practical Issues for Physician Practices*, 2017 HEALTH L. HANDBOOK 13 (May

the long term, efficiencies brought about through digital innovation can lower costs for patients and insurers, decreasing the financial burden of administrative overhead on the healthcare delivery system.[19]

Patient portal adoption also gathered steam as part of the wider consumer information access movement.[20] The increasing rate of digitization has increased the power of the consumer and the competition for consumers' time and money.[21] Consumers, generally, have come to desire easy, on-demand access to their care records.[22] Similarly, consumers wish to have transparent access to their health plan's claims information.[23] As a result, insurers, like providers, have implemented patient portals with virtual unanimity to provide consumer access to the information they demand.[24]

B. SCOPE AND VALUE OF HEALTH RECORDS

Health records are an intrinsically ubiquitous and valuable set of data, leaving their owners vulnerable to multiple frauds, thefts, and other unpleasantries if left exposed.[25] Health records

2017) (discussing the advantages of using mobile phones and applications to access patient care).

[19] *See id.*; *see also* Mansuri, *supra* note 10 and accompanying text (discussing the combination of public and private economic efficiency, demand-based, and grant incentives resulting in shifting the market balance heavily toward the adoption of full-service patient portal suites); Otte-Trojel, *supra* note 12, at 2 (noting that The Meaningful Use requirement "stick" all but ensured near-total adoption of patient portals in satisfaction of the EHR requirements); *What Physicians Need to Know About Patient Portals*, AMA WIRE (July 7, 2015), https://wire.ama-assn.org/practice-management/what-physicians-need-know-about-patient-portals ("Patients are used to accessing information online immediately, from checking their bank balance to booking travel. Physicians can tap into this expectation using patient portals.").

[20] *See generally* William B. Lober & Janine L. Flowers, *Consumer Empowerment in Health Care Amid the Internet and Social Media*, 27 SEMINARS IN ONCOLOGY NURSING 169, 174 (2011) (discussing how social trends are visible in the integration of information and communication technologies into health care, in both searching for and sharing information on the internet).

[21] *See id.* at 170.

[22] *See id.* at 176.

[23] *See* Rick Krohn, *The Consumer-Centric Personal Health Record—It's Time*, J. HEALTHCARE INFO. MGMT., Feb. 2007, at 20–21 (finding that "[w]hile surveys confirm that most of the general population is unaware of PHR systems, they also reveal consumer and patient interest in their potential value").

[24] *Id.* at 21.

[25] *See* Caroline Hunter & Jim Finkle, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, REUTERS (Sept. 24, 2014),

have long been recognized as vulnerable, valuable targets worth ten to twenty times that of a stolen credit card number.[26] Data stolen from health records includes personally identifiable information (PII) and PHI, with names, diagnoses, payer IDs, financial information, summaries of care, contact information, and dates of birth potentially compromised in a breach of such a record.[27]

This valuable data is most commonly used in insurance fraud because of its difficult-to-audit nature compared to other financial frauds.[28] A thief can abscond with one's insurance name, date of birth, enrollee number, and group number, and, in theory, run huge bills against their victims—the insurer and the enrollee, purchasing and reselling, or using themselves, medical equipment and drugs.[29] Such an actor can also falsify provider numbers and file bogus claims against the insurer.[30] This sort of fraud has increased exponentially as technology has developed, though most anti-fraud efforts on the part of government and insurers remain focused on fraudulent provider billing practices.[31] Often, the first sign of this fraud to a patient is not a strange line item from the credit card company or a call from a biller, but a months-out call from a medical collections agent, unordered service line items in the oft-discarded and unread payer Explanation of Benefits notices, or some other form of notice from the health insurer.[32] Cases of medical identity theft cost the average victim around $13,500 to fix, with an estimated 2.32 million victims.[33] The total cost to the economy for medical

https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 ("Security experts say cyber criminals are increasingly targeting the $3 trillion U.S. healthcare industry.").

[26] *See id.*

[27] *See id.*

[28] *See* FED. TRADE COMM'N, MEDICAL IDENTITY THEFT (Aug. 2012), https://www.consumer.ftc.gov/articles/0171-medical-identity-theft (discussing ways to report and recover from medical identity theft).

[29] Hunter & Finkle, *supra* note 26.

[30] *See id.*

[31] *See id.*

[32] *See* FED. TRADE COMM'N, *supra* note 28.

[33] *See* Dan Munro, *New Study Says Over 2 Million Americans Are Victims of Medical Identity Theft*, FORBES (Feb. 23, 2015), https://www.forbes.com/sites/danmunro/2015/02/23/new-study-says-over-2-million-americans-are-victims-of-medical-identity-theft/#470344ee15a0; *see also* Kelli B. Grant, *How to Protect Yourself From Medical Identity Theft*, CNBC

identity theft was estimated at $41.3 billion in 2012, or around 1.5% of 2010 total medical spending in the United States.[34]

Health data can be and is used for more classic forms of identity theft, due to the trove of information a patient record can represent.[35] The health sector had a plurality, in comparison to all other major sectors of domestic economic activity, of total incidents of identity theft reported in one report.[36] The data stolen from healthcare providers did not solely include patient PHI: other lost data includes PII, financial, payment, and authentication data.[37] Leaked PII and payment information are used to run fraudulent charges against the victim's credit cards, open new lines of credit in the victim's name, file false tax returns, assume the victim's credentials to gain access, sell the victim's data to others who can engage in frauds, and undertake other activities in the victim's name.[38] If the PII or PHI leaked includes the victim's relative's name or other personal information, data criminals can use that data to force their way into the victim's accounts through deriving answers to security questions, such as his mother's maiden name, his first child's name, last four digits of his social security number, or other identity verification queries that can be derived in such a fashion.[39]

(Nov. 10, 2016), https://www.cnbc.com/2016/11/08/how-to-protect-yourself-from-medical-identity-theft.html.

[34] *See* Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS (Aug. 25, 2016), https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/; *see also Health Care Costs: A Primer,* KAISER FAMILY FOUNDATION (May 1, 2012), https://www.kff.org/report-section/health-care-costs-a-primer-2012-report/ (discussing U.S. healthcare spending as a portion of the economy generally).

[35] *See* NUMAAN HUQ, FOLLOW THE DATA: DISSECTING DATA BREACHES AND DEBUNKING MYTHS 13 (2015), https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf (finding that hackers use health data to "gain access to resources or services, apply for credit cards or loans, register fake accounts, file fraudulent tax returns to collect rebates, and other activities without the victim's knowledge or consent.").

[36] *See id.* (finding that the healthcare sector was most affected by data breaches, followed by the government and retail sectors).

[37] *See id.* at 14.

[38] *Id.* at 13, 22.

[39] For a discussion of the possibilities of derivative identity theft like the hypothetical posed in the accompanying text, see Mike Timmermann, *Why You Should Change All of Your Security Question Answers Right Now*, CLARK (Oct.

Health record loss threatens the integrity of one's person at the most extreme end of data-enabled personal information disclosure.[40] Breach of protected health records poses a threat to one's person in two primary ways: first, the classical safety risks of release of PII; second, release or compromise of a patient's PHI, and the consequences such exposure brings. The first threat resembles the classic dangers of PII release, or "doxxing," in online parlance.[41] Releasing a person's name and home or job address renders them targets for cyberbullying, stalking, and extortion.[42] One of the more extreme examples of threats to the person extending from PII release is "swatting," a form of extreme harassment where a false emergency is reported at the victim's home or office and an often fully-armed police response follows.[43] Victims may then be surprised at gunpoint, as in the case of California state senator Ted Lieu in 2013.[44] This harassment may result in the injury or death of the victim.[45] Release of PII obtained from health portals carries as much risk

6, 2017), http://clark.com/consumer-issues-id-theft/security-questions-challenge-answers-hackers-why-you-should-change/.

[40] *See* Huq, *supra* note 36, at 13 (showing healthcare industry to have the most breaches of any industry); Hunter & Finkle, supra note 26 (discussing value of health information). See *supra* sections I.A and I.B for a discussion of the large amount and variety of personal and identifiable information stored with medical providers through EHR and patient portal systems.

[41] *See* Anneliese Mahoney, *Doxxing and Swatting: New Frontiers in Online Harassment*, LAW STREET (May 8, 2017), https://lawstreetmedia.com/issues/technology/doxxing-swatting-online-harassment/ (explaining that "doxxing," from the word "document," is the release of personal information).

[42] *See id.*; *see also* Ana Dascalescu, *Doxxing Can Ruin Your Life. Here's How (You Can Avoid It)*, HEIMDAL SECURITY (Jan. 3, 2018), https://heimdalsecurity.com/blog/doxxing/#doxxingnudes (noting various instances of doxxing).

[43] *See* Mahoney, *supra* note 41.

[44] *See id.*; Patrick McGreevy, *Senator with Anti-Swatting Bill is Victim of Hoax Emergency Call*, L.A.TIMES (Apr. 19, 2013), http://articles.latimes.com/2013/apr/19/local/la-me-pc-senator-swatting-20130419 (recounting how a hoax text message prompted an armed police response to a purported shooting at the Senator's home).

[45] For example, after a false report of a hostage situation, armed police shot a victim of swatting with rubber bullets, resulting in broken bones and bruising. *See* Ben Kentish, *British Man Charged After US Gamer is Shot by Swat Police Following Hoax Terrorism Call*, INDEPENDENT (Apr. 10, 2017), https://www.independent.co.uk/news/uk/home-news/robert-mcdaid-charged-tyran-dobbs-swatting-hoax-call-swat-terrorism-maryland-shot-gun-explosives-a7677071.html.

of crimes against the person as release of PII from any other source.[46]

The second threat against the person that results from a release or compromise of health records specifically involves sensitive PHI. PHI can be used as a mode of blackmail and extortion.[47] Medical records include sensitive information, like diagnoses of psychological conditions, sexually transmitted diseases, cancer, and other compromising information.[48] Release of this information can at the least cause embarrassment, and at the worst feed character assassination of more public persons.[49] If a patient portal system were sufficiently compromised and an actor had particularly bad intent, these systems could be used to directly harm a person in the medical context as well.[50] For example, a bad actor with access to a targeted patient's medical condition, prescription, and care records could edit those records to reflect the information they wanted to see. Physicians rely on the accuracy of their electronic health records of their patients to prescribe medication and undertake courses of treatment.[51] A bad actor could, in theory, edit that record, misleading a physician to undertake a course of treatment that could seriously harm a patient because of the compromised data's inaccuracy.[52]

[46] *See, e.g.*, Huq, *supra* note 3536 at 13; *Personally Identifiable Information: HIPAA Best Practices*, VIRTRU (May 20, 2016), https://www.virtru.com/blog/personally-identifiable-information-hipaa/.

[47] Mariya Yao, *Your Electronic Medical Records Could Be Worth $1000 To Hackers*, FORBES (Apr. 14, 2017), https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#584686e350cf.

[48] *Id.*

[49] *Id.* Yao discusses use of falsified PHI to suggest Hillary Clinton was not physically able to hold office, thus potentially undermining her presidential bid in 2016. *Id.*; *see also* Robert Farley, *Fake Clinton Medical Records*, FACTCHECK.ORG (Aug. 16, 2016), https://www.factcheck.org/2016/08/fake-clinton-medical-records/.

[50] Clarke & Youngstein, *Cyberattack on Britain's National Health Service — A Wake-Up Call for Modern Medicine*, NEW ENG. J. OF MED., Aug. 3, 2017, at 411.

[51] *See* discussion *supra* note 10 and accompanying text.

[52] This is far from the realm of speculative science fiction. See the discussion of medical device hackability concerns and the transferability of those harms in principle to patient portals, which play a similarly crucial role in patient care, *supra* note 10.

C. PRIMER ON DISTRIBUTED APPLICATION SECURITY METHODS

Distributed application security measures form a constantly-evolving component of information security.[53] A variety of methods exist to strengthen applications in the face of attack, many of which are balanced on a cost-benefit analysis of their implementation in specific applications, as well as on the competency of a particular development team.[54] In the present technological environment, the most notable and widely-implemented method of securing application communications is in-transit encryption, commonly over the Secure Sockets Layer (SSL) protocol.[55] SSL is a silent-running method of application security which encrypts communications when they are in transit between a client's computer and a provider's server, effectively preventing data eavesdroppers from unscrambling that data and leeching off the unguarded information—which may include PHI and PII.[56] Without SSL encryption, an attacker could listen in on communications between the provider's server and the patient's machine, enabling her to siphon off all kinds of personal data.[57] SSL is one of the few specific federal cybersecurity regulatory requirements presently in effect.[58] For example, the U.S. Department of Defense is required to use SSL to store protected information.[59]

Another primary form of data security is the encryption of data on the server itself through hardware and software. This

[53] *See generally* J.M. Olejarz, *The Evolving Cyberthreat*, HARV. BUS. REV., Nov. 2015, at 150, 151 (arguing that a more dynamic security strategy sharing platform is necessary to keep up with equally dynamic cyberthreats).

[54] *See generally* Mohammad S. Jalali & Jessica P. Kaiser, *Cybersecurity in Hospitals: A Systematic, Organizational Perspective*, J. MED. INTERNET RES., May 8, 2018, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/ (discussing how hospitals decide what cybersecurity measures to pursue).

[55] *See id.; see also Everything You Need to Know About SSL Certificates*, VERISIGN, https://www.verisign.com/en_US/website-presence/website-optimization/ssl-certificates/index.xhtml (last visited Feb. 5, 2019). SSL presence is often indicated by a "lock" indicator in many internet browsers.

[56] *See id.*

[57] *See id.* (describing SSL as enabling a "private conversation just between the two intended parties").

[58] *See* KATE CHARLET, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, UNDERSTANDING FEDERAL CYBERSECURITY 6 (2018) (noting that federal agencies are required to develop and report generally on cybersecurity measures). There is no mention of specific programs or technologies required by the federal government; *see also id.*

[59] 32 C.F.R. § 505.2(c)(3) (2019).

type of encryption scrambles the data so that someone with access to the provider's server cannot arbitrarily gain access to the data stored on it.[60] For web applications, decryption (for data presented to the user) and encryption (for data submitted by the user or provider to or through the application) may be handled on the "front end" (i.e., decrypted or encrypted on the user's machine) or the "back end" (where operations are handled on the server and the results presented through an encrypted SSL pipe).[61]

Additional measures exist for securing web-based applications that are of particular relevance to PHI-sensitive uses.[62] Multi-factor authentication requires the end user to use another method, other than their username and password, to log in to a computer or site.[63] User role authentication and control prevents users from accessing data that is not theirs, editing data which they should not be editing, or gaining privileges they should not have.[64] This kind of authentication could have prevented the sort of breach Molina experienced.[65] Another method—enforcing updates to system and application software, or "patching"—is often deployed to close known security vulnerabilities,[66] a commonly-touted best practice that the

[60] *See* Caroline Sanders Reach, *Client Data in the Cloud*, 28 CHI. B. ASS'N REC. 44, 49 (2014).

[61] *See generally* Eric Limer, *Mega's Clever Encryption Will Protect You, But Mostly Kim Dotcom*, GIZMODO (Jan. 19, 2013), https://gizmodo.com/5977265/how-megas-encryption-will-protect-you-but-mostly-kim-dotcom.

[62] *See generally* ORACLE, HITECH'S CHALLENGE TO THE HEALTH CARE INDUSTRY (2011), https://www.oracle.com/assets/owp-security-hipaa-hitech-522515.pdf.

[63] *See* Info. Tech. Lab., *Back to Basics: Multi-Factor Authentication (MFA)*, NAT'L INST. OF STANDARDS AND TECH. (Nov. 22, 2016), https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication. This sort of authentication most commonly includes a mobile phone app response or entry of a code sent via text message, but can include facial recognition, smartcards, biometrics, and other forms of authentication. *See id.* An attacker thus would not be able to access someone's portal account merely with their password but would have the added challenge of taking whatever device acts as the second authenticator, or cracking a second-factor biometric. *See id.*

[64] *See Azure Data Security and Encryption Best Practices*, MICROSOFT (Dec. 18, 2018), https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices.

[65] *See generally id.*; *see also* Davis, *supra* note 1 and accompanying text.

[66] *See* Dan Goldberg & Addy Baird, *As Cyber Attacks Rise, Hospitals Seek to Protect Medical Records*, POLITICO (Apr. 14, 2016),

healthcare industry in particular rarely follows.[67] Training users on system use and compliance, in addition to in-built data validation, can prevent potentially catastrophic user errors.[68] Out-of-date software, which many hospitals and clinics may use,[69] contains vulnerabilities which are often patched on newer releases; these (undefended because of legacy software) vulnerabilities are known to attackers, who can make an easy grab for information.[70] Thus, the medical sector is an easier target for information criminals.[71] Ensuring that software is regularly updated would go far in protecting hospitals and clinics from these simple attacks.[72]

D. EVOLUTION OF DATA SECURITY AND HEALTHCARE DATA STATUTES

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[73] forms the cornerstone of the current healthcare

https://www.politico.com/states/new-york/albany/story/2016/04/as-cyber-attacks-rise-hospitals-seek-to-protect-medical-records-067223.

[67] *See* Mike Schrock, *Unpatched Software Vulnerabilities a Growing Problem*, OPSWAT (Apr. 14, 2015), https://www.opswat.com/blog/unpatched-software-vulnerabilities-growing-problem (noting that 44% of breaches in 2014 exploited vulnerabilities that could have been patched via software updates two to four years prior); Steve Manzuik, *How Hospitals Are Getting Hacked and How to Prevent It From Happening To You*, HEALTH IT OUTCOMES (May 26, 2016), https://www.healthitoutcomes.com/doc/how-hospitals-are-getting-hacked-and-how-to-prevent-it-from-happening-to-you-0001 (listing outdated software and hardware as the major vulnerabilities in hospital cybersecurity).

[68] *See generally* Goldberg & Baird, *supra* note 66.

[69] Software often goes unpatched or underpatched in medical contexts due to a combination of lack of financial resources, dependence on software only compatible with older versions of system software or other interdependent programs, or a perceived lack of need to upgrade by key stakeholders. *See, e.g.*, Manzuik, *supra* note 67; Damien Gayle et al., *NHS Seeks to Recover from Global Cyber-Attack as Security Concerns Resurface*, THE GUARDIAN (May 13, 2017), https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack; Noel Towell & Aisha Dow, *Obsolete, Outdated Software puts Victorian Hospitals and Police at Risk of Cyber Attacks*, THE AGE (Nov. 29, 2017), https://www.theage.com.au/national/victoria/obsolete-outdated-software-puts-victorian-hospitals-and-police-at-risk-of-cyber-attacks-20171129-gzv9ov.html.

[70] *See* Manzuik, *supra* note 67.

[71] *See id.*

[72] *See id.*

[73] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

data regulatory scheme.[74] HIPAA effectively acts as the health sector catch-all statute, authorizing the promulgation of health sector regulations for covered entities (i.e. insurers, billing clearinghouses, and providers).[75] HIPAA requires that the Secretary of Health and Human Services ("Secretary") and the Attorney General issue guidelines to coordinate the enforcement, investigation, and evaluation of health plans to control fraud and abuse.[76] In so doing, it protects the individual's privacy and information confidentiality throughout the course of investigation.[77] HIPAA's information regulating muscle derives from the Administrative Simplification part of the Act, which sets out broad definitions of health information and requires the Secretary to promulgate regulations and standards to safeguard the security of health information and transactions.[78] The Act also provides for regulatory and criminal penalties for noncompliance or knowing wrongful disclosure of "individually identifiable health information[,]" while refusing to preempt other causes of action that may arise out of such misappropriation or noncompliance.[79]

The previously discussed HITECH Act, enacted as part of the wider American Reinvestment and Recovery Act of 2009, established an Office of the National Coordinator for health information technology and created a grant program to advance

[74] *See* Aaron P. Sohaski & Jordan B. Segal, *Litigation in a HITECH World*, 95 MICH. B.J. 52, 52 (Nov. 2016); *see generally* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 683–84 (2007).

[75] *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, § 1172, 110 Stat. 1936 (1996); *see also* Juliana Bell, Comment, *Privacy at Risk: Patients Use New Web Products to Store and Share Personal Health Records*, 38 U. BALT. L. REV. 485, 488 (2009) (citing Deborah F. Buckman, *Annotation, Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. Fed. 133 (2004). In essence, anyone in the direct chain of data processing or use between patient and provider, though not necessarily third parties outside that chain like fitness data amalgamators or user-initiated application portals outside the provider-patient scheme, is covered and must ensure the safety of patient data inside and outside the facility. *See* Sohaski & Segal, *supra* note 74.

[76] *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, § 1128C(a)(3)(B), 110 Stat. 1936 (1996) (codified at 42 U.S.C. 1320a–7c).

[77] *See id.*

[78] *See id.* §§ 1172, 1173, 1175 (codified at 42 U.S.C. § 1320d-1–d-4).

[79] *Id.* §§ 1176, 1177 (codified at 42 U.S.C. § 1320d-5–6).

"health care information enterprise integration[.]"[80] HITECH also established the aforementioned carrot-and-stick incentives to shift providers to EHRs,[81] created a policy committee empowered to recommend national health infrastructure developments,[82] and created regional centers of excellence to disseminate best practices to health organizations.[83]

HITECH's substantive amendments to HIPAA came through its Part D privacy modifications. HITECH requires covered entities to implement policies and procedures to "prevent, detect, contain, and correct security violations[,]" perform risk assessments, and implement sanction, risk analysis, review, and disaster recovery policies.[84] Further requirements include the implementation of facility security plans, sensitive information disposal plans, and access control and authentication measures.[85]

HITECH further requires that a company subject to a data breach notify the users impacted of the scope of the breach within sixty days, with breaches involving more than 500 records to be reported to the Secretary of Health and Human Services (which the Department may then disclose as an incident) unless law enforcement deems notification to be a threat to national security or criminal investigations.[86]

[80] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Title 8, 123 Stat. 115, 179 (2009) (codified in scattered sections of 19, 26, 29, and 42 U.S.C.); 42 U.S.C. § 300jj-11 (establishing Office of the National Coordinator); 42 U.S.C. § 17912 (establishing grant program).

[81] *See* Terry, s*upra* note 14, at 46 and accompanying text.

[82] 42 U.S.C. § 300jj-12(a) (2016).

[83] 42 U.S.C. § 300jj-32(c)(1) (2009).

[84] *Id.* at §§ 258, 260; 45 C.F.R. § 164.308 (2019).

[85] 45 C.F.R. §§ 164.310(a)(2)(ii), (a)(2)(iii), and (d)(2)(i) (2019).

[86] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402, 123 Stat. 115, 261–62. Note that a breach is distinguishable from a vulnerability in that a vulnerability involves a *possibly* exploitable security fault in an application, whereas a breach is an *actually-used* vulnerability to affect some end, most often malicious, such as stealing data. *See generally* Sharon Durant, *Types of Security Threats: The Differences Between a Vulnerability, Threat and Breach?*, DIGITAL WEST (May 19, 2015), https://blog.digitalwest.com/blog/what-is-the-difference-between-a-security-vulnerability-threat-and-breach. As such, breach notification would not necessarily come into play on discovery of a vulnerability that has not been used; nonetheless, breach notifications may be sent if a party thinks it to be reasonably prudent, especially if they have indication that there is some not insubstantial chance that a vulnerability may have been exploited. *Cf.* 45 C.F.R. § 164.404 (2019) ("A covered entity shall . . . notify each individual whose

Disclosures of PHI to carry out business operations are limited by the Act to the "minimum necessary" data.[87]

The weight of HIPAA and HITECH's regulatory text is promulgated through HIPAA Omnibus Regulations.[88] The regulations provide for civil monetary penalties for breaches of the Act's regulations,[89] allowed business uses for protected health information,[90] and rules relating to notification of breaches to the public.[91] The section of regulations pertaining specifically to privacy and protection of electronic health information and records specifically calls for "[f]lexibility of approach," enabling covered entities to use any "reasonabl[e] and appropriate" security measures as long as they "ensure the confidentiality, integrity, and availability" of all EHRs, protect against reasonable threats to that data's security, and protect against banned uses or disclosures of EHRs.[92] This flexibility comes with certain mandatory minimum standards designed to enforce some sense of security competence on covered entities, including a requirement for risk assessments, and

unsecured protected health information has been, or is *reasonably believed* by the covered entity to have been accessed . . . as a result of such a breach.") (emphasis added).

[87] § 13402, 123 Stat. at 265.

[88] *See*, *e.g.*, 45 C.F.R. § 160.101 (2017) (describing the purpose of 45 C.F.R. § 160 in part as implementing HIPAA and HITECH). This regulation only received its real enforcement and regulatory teeth from the 2009 HITECH Act amending HIPAA. *See* Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 608–10 (2014). This particular set of regulations is often called the Security Rule. *Id.* For more on the Security Rule, see Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH. L.J. 1523, 1556 (2009).

[89] *See* 45 C.F.R. § 160.404 (2019) (establishing a per-violation window of $100 to $50,000, and an added penalty of not more than $1.5 million for repeated, identical violations in the same year).

[90] *See* 45 C.F.R. § 164.502 (2019). This regulation allows for disclosure, e.g., to the individual, for purposes including treatment, operations, or payment, and in compliance with the rest of the regulation, among other uses. *Id.*

[91] *See* 45 C.F.R. § 164.404 (2017) (requiring the notification to be in "plain language," describe the event and the types of information breached, steps individuals should take to protect themselves, a description of what the entity is doing to remediate the breach and provide free-of-charge contact information for concerned customers). Section 164.406 requires notification of a large breach (more than 500 residents of a State or other jurisdiction) to be disseminated to the media and the Department of Health and Human Services within 60 days. *See* 45 C.F.R. § 164.406 (2019).

[92] 45 C.F.R. § 164.306 (2019).

implementation of reasonable and appropriate safeguards pursuant to the broader Privacy Rule.[93]

A proposed piece of legislation, the Improving Health Information Technology Act, was a tabled piece of bipartisan legislation in 2016 designed to address the shifting cybersecurity concerns in the healthcare market.[94] The legislation introduced more concrete requirements on healthcare information technology, including a ban on information blocking in particular applications and a general requirement of unimpeded and open access to consumer health information.[95] The bill provided for the creation of a partially-voluntary, standardized rating system for health IT products drawing from providers, IT professionals, patients, security and design experts, manufacturers, and others.[96] These ratings would evaluate platform openness, security, usability, and conformity to standards.[97] Products receiving a one-star rating from an independently-convened rating panel would be decertified, as would products not reporting appropriate information to the Department of Health and Human Services in a timely manner.[98] Product ratings would be available for public review on the Department website.[99] Decertification results in that provider being exempted from Medicare's Meaningful Use Incentive program.[100]

II. ANALYSIS

This part discusses ways the present Acts, regulations, and court holdings emphasize the importance of the principle of healthcare record privacy through strong enforcement provisions. It will then turn to an examination of how those laws fail to provide for an adequate framework for disseminating,

[93] *See* Pasquale & Ragone, *supra* note 88, at 608.

[94] *See* S. 2511, 114th Cong. (as reported by S. Comm. Health, Education, Labor, and Pensions, 2016).

[95] *Id.* § 3(a).

[96] *Id.* § 3009A. Also of note is the section directing the Secretary to draw from the expertise of NIST in developing these standards. *See id.*

[97] *See id.* § 3009A(b)(4)(A) (listing categories of reporting criteria for health information technology products).

[98] *Id.* § 3009A(g)–(i).

[99] *Id.* § 3009A(k).

[100] CONG. RESEARCH SERV., S.2511 IMPROVING HEALTH INFORMATION TECHNOLOGY ACT (2016), https://www.congress.gov/bill/114th-congress/senate-bill/2511.

enforcing, and unifying healthcare record security best practices as a component of personal and national security, exposing resource-strapped or careless providers and insurers to extensive potential liabilities.

A. HIPAA AND ITS HITECH AMENDMENTS LAY IMPORTANT GROUNDWORK FOR DATA PRIVACY AND SECURITY.

HIPAA and its amendments provide an important line of protections for valuable health information.[101] While the piecemeal, sectoral approach to information security and privacy results in an inconsistent patchwork of regulation across sectors, HIPAA and HITECH create a somewhat powerful enforcement regimen for the release of patient protected health information and personally identifiable information, and are largely successful at creating the statutory framework for a comprehensive, sector-specific information governance baseline regimen in the healthcare space.[102]

HIPAA derives its main enforcement power from the promulgations of administrative procedures through the notice and comment rule processes.[103] Its broad definition of health information and health care provider, health plan, and health care clearinghouse appropriately includes most segments of the healthcare services and delivery sector. This includes companies without a direct relationship to the patient on the processing or use end, like certain business associates and subcontractors.[104]

[101] *See* Shoaski & Segal, *supra* note 74; *see also* James Titcomb, *Windows 95 at 20: How Bill Gates' Software Changed the World*, TELEGRAPH (Aug. 24, 2015), https://www.telegraph.co.uk/technology/microsoft/windows/11817065/Twenty-years-ago-Microsoft-launched-Windows-95-changing-the-world.html (establishing that time period as the first major period of consumerization of the internet with the advent of Windows 95 (with Internet Explorer) providing many people with their first taste of internet browsing).

[102] *See* Bell, *supra* note 75; *see also* Hoffman & Podgurski, *supra* note 88, at 1556; *see also* Pasquale & Ragone, *supra* note 88, at 607–09. Notably, however, HIPAA's *only* enforcement mechanism comes from enforcement by the Secretary of Health and Human Services, lacking a private right of action, which has left the regulatory and statutory framework open for substantial criticism in its end efficacy from within the federal government itself and some sectors of the healthcare legal community. Hoffman & Podgurski, *supra* note 88, at 1556–57.

[103] *See* § 262, 110 Stat. at 2023–28; *see* Hoffman & Podgurski, *supra* note 88, at 1556–57.

[104] *See* §§ 261–62, 110 Stat. at 2021–23 (describing health information as all data created or received by a covered entity and relating to the physical or

The uniform inclusion of public (e.g. veterans', Medicare, and Medicaid) and private (group and individual) health plans—the primary payer side of the American healthcare model—covers much of the sensitive information health plans carry that is distinct from the information health care providers carry, namely financial information, health questionnaires, cross-provider referrals and diagnostic codes, and the personal information of covered households.[105] Their inclusion is not overbroad, as recent breaches have aptly demonstrated: health payers process protected health information that is as significant as the information processed by the providers in their network, and the risks of exposure of that information justify their inclusion in the legislation.[106]

Moreover, the wide inclusion of health care clearinghouses—institutions that manage a component of the health care data processing business, like billing or coding vendors—serves to protect patient information from disclosure when working outside the somewhat-direct payer-provider relationship.[107] Requiring data clearinghouses to abide by the regulations applied to their clients provides incentives for providers and payers to carefully select vendors to work with their sensitive client information, and ensures that all phases of the traditional health care business model are adequately seeking to protect patient data.[108]

The current regulation, through HIPAA, of not only the health care records themselves, but the records relating to payment and provision of care, recognizes the risks that the present information model presents to patients.[109] The risks of disclosure of health payer information ancillary to the leaking of patient health records, such as insurance member and group IDs, credit card numbers, and routing information, make the economic pain of an unauthorized release of health information much worse due to the extensive costs of healthcare benefit and

mental health of an individual or the provision or payment of their care); *see also* Pasquale & Ragone, *supra* note 88, at 608.

[105] §§ 261–62, 110 Stat. at 2021–23; *see supra* notes 4, 6, 24 and accompanying text.

[106] *See supra* notes 1–6 and accompanying text; *see also infra* note 111.

[107] *See* § 262, 110 Stat. at 2021.

[108] *See* Austin Rutherford, *Byrne: Closing the Gap Between HIPAA and Patient Privacy*, 53 SAN DIEGO L. REV. 201, 212 (2016) (discussing the expansion of entities subject to HIPAA).

[109] *See* § 262, 110 Stat. at 2022.

classical financial frauds.[110] As financial crimes against healthcare companies are comparatively difficult to detect in cases where identity theft is the root cause, the Act's broad inclusion of financial information under its ambit of protection is a response appropriately measured to the risks of financial data leakage, even in the modern computing era.[111]

HIPAA's stringent sanctions serve to provide an appropriately strong incentive for health care companies to focus on data security and the privacy of their patients outside of prior-existing causes of action. The regulations promulgated under the Act call for severe penalties for failure to comply with the privacy requirements of HIPAA, with up to $50,000 in penalties assigned per violation and $1.5 million assigned for repeat, identical violations during a calendar year.[112] The massive potential for liability for failure to comply with federal privacy requirements imputed by the Act and its regulations in this case provide a reasonable penal incentive for companies to safeguard the privacy of their patients' information.[113] The flexibility in the regulation for penalty value assignment enables the Department of Health and Human Services to scale their assessment of fees to the severity of the breach while providing enough of a dollar figure amount to facially dissuade companies from playing loosely with protected information.[114]

In a world shrinking by the proliferation of big data and the resulting ability to extrapolate based on a few bits of data, the combined breadth of regulation and potential severity of sanctions continue to reflect this changing reality.[115] Though individual health records pose enough of a risk to an individual's privacy and financial integrity in isolation, the amalgamation of data available to providers in the present technological environment, and, thus, stored *en masse* on health service

[110] *See supra* note 26 and accompanying text.

[111] *See supra* note 31 and accompanying text; *see also* Phuong Tran, *Anthem Data Breach Will Cost Record Fine of $115 Million*, PAUBOX (June 26, 2017), https://www.paubox.com/blog/anthem-data-breach-will-cost-115-million (providing information on liabilities extending out of a HIPAA violation).

[112] 45 C.F.R. § 160.404 (2019).

[113] *See* Pasquale & Ragone, *supra* note 88, at 622 (describing civil penalties as "important incentives for proper behavior").

[114] *Cf.* 45 C.F.R. § 160.404 (2017) (providing civil money penalties ranging from $100 to $50,000 per violation).

[115] *See*, *e.g.*, *id.*; §§ 261–262, 110 Stat. at 2021–23; *see also* Rutherford, *supra* note 108, at 212–13.

providers' and payers' databases, provides a far greater level of danger in the event of their release.[116] The morass of data now stored as part of individual health records can easily decode individuals' living situations, states and patterns of health, and financial information, among other data.[117]

An act amending HIPAA, HITECH, discussed previously,[118] began attempts to modernize HIPAA for the digital age where necessary.[119] One such needed modernization was in enacting breach notification provisions, which struck an appropriate balance on data protection while comporting with other sectors' regulations, providing for uniform requirements to protect consumers.[120] Requiring consumers to be notified of breaches, and perhaps substantial vulnerabilities where a vulnerability carries substantial risk of breach, within sixty days absent the presence of a finding from law enforcement officers that notification would impede a criminal investigation or damage national security, and to report breaches to the Department of Health and Human Services for disclosure acknowledges the aforementioned ballooning data (with the risks and liabilities contingent on that ballooning) of health providers and payers.[121] With the Act recognizing the digitization of data and consequent compounding of pieces of data into comprehensive, centralized masses of files, the legislation's breach notification requirements enable consumers to be protected from the multiple types of fraud to which they are now more vulnerable.[122] Mandating disclosure of such breaches requires transparency and accountability to customers, officials, and the public regarding the effectiveness of a company's data security regimen and the potential for risk in doing business with that company.[123]

[116] *See* discussion *supra* Section I.B.

[117] *See id.*

[118] *See* discussion *supra* Section I.A.

[119] *See* Hoffman & Podgurski, *supra* note 88, at 1556–57.

[120] *See*, *e.g.*, § 13402, 123 Stat. at 261–62; *see also* Pasquale & Ragone, *supra* note 88, at 652 ("The post-HITECH landscape will increasingly balance these [privacy] concerns with the goals of innovation, access, and cost-control.").

[121] *See* discussion *supra* Section I.B; *see also* Rutherford, *supra* note 108, at 212–13.

[122] *See* Rutherford, *supra* note 108, at 213 (noting that data breaches are increasingly common over the years).

[123] *See* Pasquale & Ragone, *supra* note 88, at 645 (arguing that intense surveillance of the data security and privacy system motivates providers to modernize their practices and increases their productivity).

Meanwhile, the breach notification requirements enable those protected consumers to, for instance, monitor their claims records and financial accounts.[124] The Act's public notice provisions also serve to cut the vectors for undetected medical benefit fraud by enabling payers to receive notice of a potential fraud problem arising out of a breach and implement countermeasures, saving all customers money through reducing losses from fraud on that plan.[125]

B. THE PRESENT LEGAL FRAMEWORK DOES NOT PROPOSE CONCRETE SOLUTIONS TO THE MODERN APPLICATION SECURITY CONUNDRUM.

Yet, with the strengths of HIPAA and HITECH noted, the present legal framework created by the Acts and their regulations exhaustively swings a punitive stick at the repairing damage end of the privacy enforcement spectrum.[126] While, through threats of penalties for failures, HIPAA tries to incentivize adoption of best privacy practices, it relies too heavily on punitive enforcement methods and voluntary cooperation; it is all stick and no carrot.[127] There is no provision for an adequate framework for actually improving privacy practices, especially in the technology realm, despite HITECH's Part D amendments.[128]

[124] *See id.* at 644–45 (noting that educating customers to evaluate whether security is reasonable is critical).

[125] *See* FED. TRADE COMM'N, *supra* note 28 (providing examples of how to correct mistakes in one's medical records when medical identity theft occurs); *see also* Hunter & Finkle, *supra* note 26 (reporting that fraud involving the Medicare program totaled more than $6 billion in the last two years).

[126] *See generally* Rutherford, *supra* note 108, at 214 (arguing that the threat of no-cap damages in tort suits would improve compliance by various entities subject to HIPAA regulation).

[127] *See* 45 C.F.R. § 160.404 (2017) (informing that HIPAA is enforced via civil monetary penalty); Pasquale & Ragone, *supra* note 88, at 645 (discussing the intense pressure the threat of enforcement action has on the industry, but also discussing, as one of the pitfalls, recalcitrance of cloud vendors due to the lower levels of enforcement action); Hoffman & Podgurski, *supra* note 88, at 1556–57.

[128] *See* Pasquale & Ragone, *supra* note 88, at 608. *See also* 45 C.F.R. § 164.310 (requiring implementation of policies to prevent, contain, and correct security violations and perform regular control and risk assessments). The wording of these regulations leaves much of the control over such requirements, and with it a large chunk of discretion, with the companies themselves in an attempt at internalizing regulation while presumably reducing the regulatory

HIPAA's use of penalties to incentivize a *lack of* breaches, while definitely a necessary component of the legislation, misses the mark on improving the practices of companies in the health care industry to prevent breaches from becoming an issue with such regularity in the first place.[129] While certain groups of measures can be taken to reduce the scope or probability of data breaches occurring from a weakness in systems or protocols, securing the underlying systems and constantly assessing and improving on those roadblocks to theft will prevent the breaches from occurring, at least in that time frame, in the first place.[130] While the present Acts adequately address the post-breach remediation phase, there is little enforceable coverage of incentivizing pre-breach activities to prevent breaches from occurring or limiting their scope for when they do occur.[131]

C. THE PROPOSED IMPROVING HEALTH INFORMATION TECHNOLOGY ACT OF THE 114TH CONGRESS BEGAN TO ADDRESS CONCERNS OVER INFORMATION GOVERNANCE BEST PRACTICES BUT FAILED TO ACCOUNT FOR ENFORCEABILITY.

The proposed, and ultimately tabled,[132] Improving Health Information Technology Act of 2016 was the first legislative

and administrative burdens of providing for some more specific actions and processes required of these covered entities.

[129] 110 Stat. 1936, 2021–23 (Aug. 21, 1996); 45 C.F.R. § 160.404 (2017).

[130] *See* discussion *supra* section I.C.; *see generally supra* note 8 and accompanying descriptions of vulnerable cybersecurity practices. The OWASP guidelines there cited, for instance, outline the vulnerabilities as pathways to the breaches which cause the problems in the first place. Computers follow a linear logic, as does the process of pulling information off computers without authorization (i.e. the breach itself). For a breach to occur, there must be such a vulnerability.

[131] While the Department does, in theory, have auditing authority, particularly through authority derived from dealings with CMS, the stretched resources of the Department have already been described as inadequate for purpose at best per the discussion and citation in Hoffman & Podgurski, *supra* note 88, at 1556–57. Regardless, audits remain a tool that, while more proactive than the remediation and penalty phase enforcement efforts described at length in this Note, still stems from reacting to a discovery of a problem as opposed to preventing those problems from occurring through adequate controls. While audits on those controls would be a good first step, the literature and discussions within these agencies make clear that this is not a process that can be improved with regulatory "sticks" and pervasiveness alone. Pasquale & Ragone, *supra* note 88, at 645–46.

[132] That is to say, set aside for no further consideration in that session or, thus far, in any further session. *See* STANDING RULES OF THE SENATE, S. Doc. No. 113-18, at 8 (1st Sess. 2013). Laying on the table has the meaning described

attempt at a partial solution to the conundrum discussed above.[133] Most notably, the Act attempted to implement standards for IT product design in certifying products for use in Medicare's Meaningful Use Incentive program.[134]

The framework proposed by the Act focuses on the exchange of health information and voluntary data-sharing arrangements instead of mandatory standards for national health technologies.[135] Coming out of committee, the Act requires the Department to merely "encourage" "voluntary certification of health information technology," effectively gutting the proposed Act of any teeth it may have had or needed to ensure that its aims were met.[136] In relegating the standardized, standards-based star rating system for health IT, which would have drawn from a multisector, multidisciplinary panel of experts in assessing, among other qualities, a health IT software package's information security and privacy protections, to a partially voluntary framework under which decertification from Meaningful Access would be the only real possible penalty and only under a fixed set of circumstances, the Act ends not far from where it began: with no real solution to the unregulated health IT development space and the problems it imports.[137]

The framework further needlessly segments pediatric and adult data handling, adding an unnecessary layer of complexity to the Act.[138] The Act provides, without explanation, for different certification standards and deadlines for various classes of patient and facility, most notably for practices supporting child health care.[139] This complication is unnecessary: children have largely the same privacy and data exchange needs and medical record specifications as adults.[140] Providing segmented

as it is a final disposition in the negative on certain substantive and subsidiary motions which affect consideration of a "main" question or matter before the Chair.

[133] S. 2511, 114th Cong. (2016).

[134] *Id.* § 2(a) at 53 ¶¶ 19–25.

[135] *See id.* § 2(b).

[136] *Id.* at § 2(b) at 56 ¶¶ 1–10.

[137] *See id.*

[138] *See id.* § 2(b) at 56 ¶¶ 17–25; *see also id.* § 2(b) at 57 ¶¶ 1–8.

[139] *See id.*

[140] *Cf.* Victoria Turk, *GDPR Could Have Unintended Consequences for Teenagers*, WIRED (May 23, 2018), https://www.wired.co.uk/article/gdpr-children-under-16-parental-consent (emphasizing that GDPR recognizes that

requirements for various medicinal specialties does not advance what should be the ultimate aim of the legislation—to provide a simple but complete framework for securing national healthcare IT infrastructure.[141] Segmenting products by specialty needlessly complicates the proposed regulatory processes in the Act and products which would be developed under its purview.

III. SOLUTIONS

A revised form of the proposed 2016 Act to empower the Secretary to promulgate regulations that secure the national healthcare technology infrastructure would move many providers toward compliance, imperfectly remediating many of the risks of data breaches at providers and payers. These solutions would balance incentivization with enforcement to create a program that promotes broad industry buy-in to its ambit.

A. REFRAME THE 2016 ACT TO ENABLE EFFECTIVE ENFORCEMENT OF ACCEPTED BEST SECURITY PRACTICES FOR THE HANDLING OF SENSITIVE HEALTH INFORMATION

One of the most glaring pitfalls of proposed amendments to healthcare privacy regulations is their focus on voluntary associations as the end of the Act's provisions for ensuring compliance with best practices for data security in the industry.[142] While any Act certainly should call for voluntary associations as part of its solutions to the healthcare IT conundrum in which the nation finds itself, any meaningful legislation and regulation would necessarily have mechanisms for enforcement contained inside their text.[143]

Mandating that all healthcare IT appliances fall under the ambit of a universal, standardized healthcare IT assessment framework set by the Department of Health and Human Services regulators after consultation with all sides of the

children merit specific protection regarding their personal data because they may be less aware of the risks).

[141] *See* S. 2511, 114th Cong. § 2(a) at 52 ¶¶ 22–25 (2016) (announcing that the goal of the Act is "the reduction of regulatory or administrative burdens relating to the use of electronic health records").

[142] *See* Pasquale & Ragone, *supra* note 88, at 645–46 (describing the recalcitrance of cloud healthcare actors to act on their own volition due to limited enforcement with no incentivizing framework separate from that).

[143] *See id.*

industry, like the framework proposed by the 2016 Act, would more effectively cover the healthcare IT subsector's products and achieve the aims of ensuring healthcare IT security and preservation of privacy. As HIPAA exemplifies, broadly defining the reach of regulation in the healthcare information realm best protects consumers from poor practices relating to their data.[144] Placing all healthcare IT under the same assessment umbrella will enable uniformity of assessment, and thus expectations, of developed software, enabling a software-producing company to ingrain developmental best practices into all their healthcare products, ensuring that all products concerning protected patient health information are accurately and adequately evaluated.[145] Maintaining a baseline of pre-set minimum threshold and target-level standards that are continuously reviewed, and then tracking compliance with their implementation, would affect the goals of the assessment framework. Ensuring this evaluation and publicizing the results as the 2016 Act proposed will increase patient confidence in the integrity of health technologies and work to protect patient privacy from the pre-breach, development and implementation stages, instead of retroactively attempting to put out the fire of a massive breach.[146]

To prevent excessive barriers to entry, innovation, and competition in the healthcare technology space for Meaningful Use-covered entities, however, any such regulation should include reasonable provisions allowing for new entrants, products, and updates to be pushed to market without undergoing a full, exhaustive screening of their vulnerabilities.[147] A process, for instance, of provisional accreditation for software that passes basic tests of security

[144] *Id.*

[145] For instance, the framework like that found in OWASP, *supra* note 8, a) shows certain universal standards are applicable across sectors and approaches to development as a baseline for best practices, and b) provides an example of such a best practice regimen, combining enumerated concrete actions with abstract programming concepts to provide for a blend of programming flexibility (depending on the use case) and certain baseline requirements common to virtually every use case. *See generally* Pasquale & Ragone, *supra* note 88, at 625–26.

[146] S. 2511; Rutherford, *supra* note 108, at 212–13; Pasquale & Ragone, *supra* note 88, at 620–23.

[147] *See* Hoffman & Podgurski, *supra* note 88, at 1565 (arguing that regulation that promotes standardization would not necessarily stifle competition).

pending a full assessment and rating, will enable new products to enter the market more efficiently while minimally compromising the security aims the proposed legislation would provide.[148]

Moreover, enabling companies to update their EHR software without that iteration not being certified would encourage companies to improve on their software's design, features, and security and privacy protections without the burdens of excessive bureaucratic review.[149] A rolling process of continuous review and improvement would serve this end as well as ensuring continued compliance with evolving best practices in the security space.[150] Providing for a regimen of regular review by HHS and re-rating by the evaluation panel of healthcare technology would balance these interests and incentivize companies to continuously improve software to prevent new security holes from plaguing older, deprecating software.[151] Such a program would need to assess the realistic resource constraints and the burdens created on HHS and other involved entities, and the Secretary ought to promulgate regulations that would effectively balance burden with benefit.

Providing for an actual enforcement mechanism for these rules, such as, at a minimum, decertification from Meaningful

[148] *See id.*, at 1570 (discussing the early stages of development of EHR technologies as opportunities to formulate best practices, and, implicitly, build on those best practices as the EHR technology develops). Thus, it follows logically that providing for entry to new technologies would provide the impetus for new best practices, though with the risk of poor products coming to the market with lesser regulation, hence the provisional component of any emerging product accreditation scheme. A middle approach between effectively walling off the marketplace of EHR software to existing, verified entrants, and providing for a lack of regulation of these pieces of software, would balance the two competing interests of security and vitality.

[149] *See id.* at 1565–66 (providing that the regulatory oversight contains a mechanism for timely approval of innovative user interface features that conflict with existing guidelines).

[150] OWASP, *supra* note 8, at 19. Regular, but not so regular as to burden development, testing, and audit teams, code review, especially in light of new best practices and vulnerabilities, is accepted as a development industry best practice. *See id.* at 3. Similarly, reasonably frequent review of software, especially that published agilely (in short, continuously-updated iterations), will keep up standards while not burdening each incremental release of software with a full-fledged external review process, which could potentially keep out, as in the case with software security patch releases, the very sort of secure design that the process would, ideally, be intended to reach across the industry board.

[151] *See id.*

Use in all cases involving EHR systems (not just on a voluntary basis) or imputing regulatory and civil liability for breaches to the software-producing and -using companies, would provide an adequate deterrence to ensure compliance with the proposed system.[152]

B. CONFIRM IN THE ACT A PRIVATE RIGHT OF ACTION FOR BREACHES OF SENSITIVE HEALTHCARE DATA

Enabling consumers to take control of their healthcare data by granting a federal right of action to those consumers against companies responsible for the negligent loss of, unauthorized access to, failure to mitigate a breach of, or lack of notification of a breach of their HIPAA-protected data would provide an additional and uniform deterrence to payers, providers, and software-makers to use properly secured healthcare software in their businesses, and to react appropriately to data breaches when they do occur.[153] Since no such uniform private right of action exists under the current federal legal framework, confirming such a right under federal law would ensure uniformity of expectation and conformity to regulation.[154] It will also protect patients from losses incurred by poor data security practices where they would have no other cause or right of action.[155]

C. STRENGTHEN PROVISIONS FOR DATA SHARING OF BEST PRACTICES IN SECURITY BETWEEN VARIOUS PROVIDERS AND INSURERS

Voluntary sharing of data relating to best practices in security and privacy of healthcare technology will strengthen the overall national healthcare security situation.[156] The design

[152] *See* Terry, *supra* note 14 and accompanying text.

[153] *See* Rutherford, *supra* note 108, at 203 (arguing that giving the harmed individuals a right of action incentivizes better compliance with HIPAA by instilling in companies a fear of sizeable damage awards).

[154] *See id.*

[155] *See id.*

[156] *See generally* OWASP, *supra* note 8. These voluntary data sharing organizations would need to implement adequate internal safeguards for ensuring that any dangerous data being discussed has a minimal risk of leaking to outsiders who would thwart the whole security purpose of these data sharing associations and groups. However, making this process a national security clearance-level accreditation or screening may prove restrictive. Since these associations would be voluntary, it would likely fall to the voluntarily-

of such a voluntary data sharing program would, ideally, involve the creation of an informal national panel of multiple subject-matter experts in a variety of healthcare technology institutions, including providers, payers, and producers advising the Department of Health and Human Services and each other on technical and administrative procedures, development techniques, policies, and design principles to secure national healthcare technologies.[157] Promoting this form of public-private and private-private partnership will foster communication between all involved parties, increasing an atmosphere of trust and collaboration already implicitly anticipated under the 2016 Act's proposed interoperability requirements.[158] The information shared here would not create a standard of care or minimum expectation on healthcare technology providers and users, but would serve to strengthen the *best* practices in the industry, creating an environment where all participants' products are able to progress in this area.[159]

associating organizations and the DHS to determine these standards reflexively based on their perceived risks, needs, costs, and opportunities.

[157] There is precedent for national security-related information technology security voluntary data sharing, such as via the Department of Homeland Security's Information Sharing and Analysis Organizations, groups with members voluntarily sharing information with one another. *Information Sharing and Analysis Organizations (ISAOs)*, DEPT. OF HOMELAND SEC., https://www.dhs.gov/isao (last visited Apr. 3, 2017). Indeed, this proposal is similar to those programs with much the same intent but designed to be formed specifically within the healthcare sector and among healthcare sector lines as would involve a broader group of stakeholders, and outside the more stringent national security clearance process as ISAOs are subjected to in determining members and information to be shared. This would reach in scope beyond only national security applications despite its implications for national security.

[158] *See id.*

[159] *But see* Pasquale & Ragone, *supra* note 88, at 645 (calling for a more mandatory approach, with best practices from any reasonable source absolutely mandated). The danger in a total approach is that it may stifle discussion of these best practices while constraining individualized development approaches. The idea is to create a strong minimum standard in the solution discussed relating to enforcement of best practices, discussed *supra* section III.A, but also to create a working group where practices can be shared such that there is a free exchange of ideas while recognizing the difference in situations between the various entities represented—that is, what works for one person at that particular table will not necessarily work for another given variation in use case, development, and architecture. The Secretary could then promulgate regulations enforcing the recommendations or outcomes of discussions of that panel.

D. CONFIRM THE SECURITY OF MEDICAL RECORDS AS A NATIONAL INFRASTRUCTURAL SECURITY PRIORITY

Finally, a responsive legislative act would confirm that medical record security is a national security priority. Though the Department of Homeland Security confirms IT and healthcare as critical national infrastructure, its discussion documents fail to outline the nexus between IT and healthcare specifically, instead focusing on the system availability of patient care infrastructure and health IT.[160] Considering the potential reach of medical records into the lives of everyday people and the harms visited upon customers in the event of their undue breach, the declaration of medical security as a component of national security is not a stretch of logic.[161] At a minimum, ensuring patients' financial security while protecting the medical payer systems from fraud constitutes a substantial enough economic risk and benefit calculation to consider healthcare technology as a component of important national infrastructure. Moreover, protecting the privacy of individuals and their medical encounters, as well as those of their families, prevents domestic and international opportunists from preying on Americans.[162]

In the spirit of enshrining medical records as a matter of infrastructural security, an ideal Act would adopt at least short-term grant provisions for ensuring the continued security of the nation's medical infrastructure, particularly patient portals' public-facing infrastructure as the most vulnerable link, addressing the concerns discussed over the "stick-only" approach currently taken to healthcare security.[163] Creating a program for competitive and need-based grants to improve medical records

[160] *Critical Infrastructure Sectors*, DEPT. OF HOMELAND SEC., https://www.dhs.gov/critical-infrastructure-sectors (last visited Apr. 1, 2016); DEPT. OF HOMELAND SEC., HEALTHCARE AND PUBLIC HEALTH SECTOR-SPECIFIC PLAN 1–4 (2016). However, the DHS does recommend that healthcare IT be strengthened from a national security standpoint through implementation of improvements to private-sector information sharing, specifically through the ISAO, as this note also suggests. HEALTHCARE AND PUBLIC HEALTH SECTOR-SPECIFIC PLAN, at 46; Exec. Order No. 13,691, 3 C.F.R. § 13691 (2015).

[161] *See* discussion *supra* section I.B.

[162] *See, e.g.*, Hunter & Finkle, *supra* note 26 (reporting that Chinese hackers allegedly had broken into one of the largest U.S. hospital operators' computer network and stolen the personal information of 4.5 million patients).

[163] *See* discussion *supra* section II.B.

software security would provide a positive incentive for product developers to create adequately secure products for use in the nation's payer and provider systems.[164] Ideally, this grant program would apply broadly, enabling grants to be used for secure systems development, secure systems implementation, and continuous operational security in live production environments, so as to address all major areas of vulnerability in the healthcare IT execution waterfall.

IV. CONCLUSION

Recent, massive data breaches of patient portals in this country have revealed areas for improvement in the nation's current piece-meal and overly focused healthcare technology regulatory framework. The relatively recent advent of patient portals as a commonplace technology, joined with the vast amounts of data stored on them and the permanently-evolving threat and risk environment surrounding digital information, particularly in the healthcare industry, reveals shortcomings in the dated provisions of HIPAA and HITECH. By adopting a public, transparent, rigorous, standards-based approach to assessing and approving healthcare software products for use, in addition to incentivizing proper developmental and pre-breach practices instead of merely punishing poor security after a breach of health records, the country will be able to adopt scientific, uniform, and measurable healthcare IT standards and requirements to ensure the protection of its patient health and financial data with sufficient flexibility to meet the needs of the foreseeable future of healthcare technology.

[164] *See* discussion *supra* section III.A.