2020

Saving the Electronic Person from Digital Assault: The Case for More Robust Protections over Our Electronic Medical Records

Danielle M. Mrdjenovich

Follow this and additional works at: https://dsc.duq.edu/dlr

Part of the Medical Jurisprudence Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Danielle M. Mrdjenovich, Saving the Electronic Person from Digital Assault: The Case for More Robust Protections over Our Electronic Medical Records, 58 Duq. L. Rev. 146 (2020).
Available at: https://dsc.duq.edu/dlr/vol58/iss1/8

This Student Article is brought to you for free and open access by Duquesne Scholarship Collection. It has been accepted for inclusion in Duquesne Law Review by an authorized editor of Duquesne Scholarship Collection.
Saving the Electronic Person from Digital Assault: The Case for More Robust Protections over Our Electronic Medical Records

Danielle M. Mrdjenovich*

I. INTRODUCTION .............................................................. 147
II. BACKGROUND .................................................................. 148
   A. HIPAA ........................................................................ 148
   B. HITECH Act .............................................................. 150
   C. Current Limitations to HIPAA and the HITECH Act .......... 151
   D. Recent Cyberattacks at Large Hospitals in the United States .. 153
   E. Why We Need Additional Protection over Our Electronic Medical Records .......... 157
III. ANALYSIS ................................................................... 158
   A. Proposed Judicial Solution: Affording Federal Constitutional Protection to Patient Medical Records .......... 159
      1. A Constitutional Right to Informational Privacy .................. 160
      2. A Constitutional Right to Dignity in Medical Decision Making ......................................................... 162
      3. A Constitutional Right to the Privacy of Our Patient Medical Records .................................................. 164
   B. Proposed Legislative Solution: Making All Addressable HIPAA Standards Required for Large Covered Entities ................................................................. 169
IV. CONCLUSION .................................................................. 174

* Danielle M. Mrdjenovich is a 2020 J.D. candidate at Duquesne University School of Law. She graduated from the Pennsylvania State University in 2014 with a Bachelor of Science in Business with a concentration in Marketing and Management. The author would like to thank Professor Jan Levine for his insights and her family and friends for their constant support.
I. INTRODUCTION

Although hospital cyber security is highly regulated by the federal government, the current federal regulations fail to adequately protect patients' electronic health information from large-scale data breaches.1 Because of the widespread use of electronic medical records in the United States, the increased threat of cyberattacks should concern every American patient.2 In fact, the United States Department of Health and Human Resources Health Care Industry Cybersecurity Task Force has described the increased threat of cyberattacks as a "key public health concern" in the twenty-first century.3 Americans should be especially concerned about the threat of hospital data breaches in the aftermath of the Equifax data breach, which affected nearly half of all Americans.4 Now that we as a country have an increased awareness about the consequences of a large-scale cyberattack, we must turn our attention to the threat of a hospital data breach.

Currently, hospital cyber security is governed by two pieces of federal legislation that work in tandem to protect patient health data: the Health Insurance Portability and Accountability Act (HIPAA)5 and the Health Information Technology for Economic and Clinical Health (HITECH) Act.6 Although federal legislation currently regulates the privacy, security, and confidentiality of our patient health information, the law must provide greater protections over our most private and most sensitive data.7 This article proposes a two-pronged approach that will result in greater protection of our electronic medical records. First, this article argues that the courts should recognize a fundamental right to our medical records' privacy. Second, this article proposes revisions to the current HIPAA laws that will provide for greater security of our electronic medical information.

2. See id.
3. Id. at 2.
II. BACKGROUND

Hospital medical records are protected by HIPAA\(^8\) and the HITECH Act.\(^9\) HIPAA laws require all health-care providers to protect all medical records’ privacy and security.\(^{10}\) If a health-care provider violates patient confidentiality, then that provider may be subject to a monetary penalty.\(^{11}\) Although these laws provide more protection over electronic medical data than most other industries in the United States, these laws have not adequately adapted to the threat of large-scale data breaches to hospitals and health insurance providers.\(^{12}\) This section will discuss the HIPAA and HITECH statutory scheme and the increased threat of cyberattacks on hospitals and health insurance providers in the United States.

A. HIPAA

HIPAA requires hospitals and health insurance providers to protect the confidentiality of all patient health data.\(^{13}\) HIPAA laws apply to all medical records in both paper and electronic format.\(^{14}\) Congress originally passed HIPAA in 1996 to improve the Medicare program under title XVIII of the Social Security Act . . . , the medicaid program under title XIX of such Act . . . , and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of uniform standards and requirements for the electronic transmission of certain health information.\(^{15}\)

When initially passed, HIPAA’s primary purpose was to expand patient access to health care and health insurance in the United States.\(^{16}\) In this original bill, however, Congress included a directive to the Secretary of Health and Human Services (HHS) to

---

15. HIPAA, 42 U.S.C. § 1320d note (Purpose Section).
submit recommendations to Congress about the appropriate standards for protecting patient health information.\textsuperscript{17} The 1996 HIPAA law also directed the Secretary of HHS to enact regulations to protect electronic health records.\textsuperscript{18} Although the privacy portion of the law was more of an afterthought, this is the portion that has gained notoriety amongst clinicians and patients.\textsuperscript{19} Thus, the modern era of hospital privacy regulation was born.

In 2000, HHS promulgated the HIPAA Privacy and Security Rules, and these rules were further modified in 2002.\textsuperscript{20} The HHS Office for Civil Rights (OCR) enforces the Privacy and Security Rules.\textsuperscript{21} These rules require “covered entities” to protect confidential patient information.\textsuperscript{22} “Covered entities” include health plans, health-care clearinghouses, and health-care providers who transmit health information electronically.\textsuperscript{23} In other words, a health insurance plan, a hospital system, or an individual doctor’s office are all “covered entities” for the purposes of HIPAA laws.\textsuperscript{24}

HIPAA also applies to any “business associates” of the “covered entities.”\textsuperscript{25} According to the HIPAA Privacy and Security Rules, a “business associate” assists a “covered entity” with “a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities . . . , billing, benefit management, practice management, and repricing.”\textsuperscript{26} Additionally, a “business associate” must comply with all HIPAA rules if it provides the “covered entity” with “legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services” and “the provision of the service involves the disclosure of protected health information.”\textsuperscript{27}

\begin{thebibliography}{27}
\bibitem{17} HIPAA, 42 U.S.C. § 1320d-2.
\bibitem{18} Id.
\bibitem{19} Berwick & Gaines, \textit{supra} note 16, at 229.
\bibitem{20} JONATHAN I. EZOR, PRIVACY AND DATA PROTECTION IN BUSINESS: LAWS & PRACTICES 145 (2012).
\bibitem{22} 45 C.F.R. §§ 160, 164 (2019).
\bibitem{23} Id. § 160.163.
\bibitem{24} See id.
\bibitem{25} Id.
\bibitem{26} Id.
\bibitem{27} Id.
\end{thebibliography}
B. HITECH Act

Passed in 2009, the HITECH Act created additional protections for electronic patient information beyond the scope of HIPAA.\(^{28}\) As our society moved into the digital age, Congress realized the need for stronger protections over our electronic medical records.\(^{29}\) The HITECH Act also included provisions designed to encourage all hospital systems to install electronic medical record systems and to convert their medical records into an electronic format.\(^{30}\)

The HITECH Act created a penalty scheme if a covered entity should accidentally disclose protected health information.\(^{31}\) Fines under the HITECH Act range from $100 to $1,500,000.\(^{32}\) The penalty scheme is based upon the severity of the privacy breach as well as the culpability of the covered entity.\(^{33}\) For example, in a large data breach, a covered entity can be subject to a fine of: $100 per record\(^{34}\) for accidental disclosures;\(^{35}\) $1,000 per record\(^{36}\) for disclosures that occurred due to a reasonable cause rather than willful neglect;\(^{37}\) $10,000 per record\(^{38}\) for disclosures due to willful neglect;\(^{39}\) or $50,000 per record\(^{40}\) for disclosures due to willful neglect if the entity fails to take corrective action following the wrongful disclosure.\(^{41}\)

The HITECH Act also includes reporting requirements mandating that the covered entity notify consumers after a data breach of any size.\(^{42}\) The Act states:

[a] covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information . . . shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the

\(^{31}\) Id. § 17939.
\(^{33}\) Id.
\(^{34}\) Id. § 1320d-5(a)(3)(A).
\(^{35}\) Id. § 1320d-5(a)(3)(B).
\(^{36}\) Id. § 1320d-5(a)(3)(C).
\(^{37}\) Id. § 1320d-5(a)(1)(B).
\(^{38}\) Id. § 1320d-5(a)(1)(C).
\(^{39}\) Id. § 1320d-5(a)(1)(D).
\(^{40}\) Id. § 1320d-5(a)(1)(F).
\(^{41}\) HITECH Act, 42 U.S.C. § 17932(a) (2012).
covered entity to have been, accessed, acquired, or disclosed as a result of such breach.\textsuperscript{43}

If the data breach includes more than 500 patient records, the covered entity must then notify the individual consumers affected by the breach as well as the Secretary of HHS and local media outlets.\textsuperscript{44}

\section{C. Current Limitations to HIPAA and the HITECH Act}

Despite offering some of the strongest cyber protections of any industry in the country, there are several limitations to the HIPAA statutory scheme.\textsuperscript{45} As a result of these limitations, patient’s electronic medical records are not being adequately protected.\textsuperscript{46} HIPAA requires a state actor, such as the OCR, to bring a claim against the covered entity in the event of a data breach—the federal regulations do not create an individual cause of action for the victims of a cyberattack.\textsuperscript{47} As a result, if a consumer’s health data has been compromised, the consumer only has two available avenues for recourse, either: (1) file a complaint on the HHS website to prompt an OCR investigation or (2) attempt to bring a tort or contract action within the state or federal court system.\textsuperscript{48}

An OCR investigation into a data breach begins when a person who suspects a HIPAA violation has occurred files a complaint with the Secretary of HHS on the HHS website.\textsuperscript{49} After receiving the patient complaint, the OCR then begins an investigation into the alleged violation.\textsuperscript{50} If the OCR determines that the covered entity did not comply with HIPAA laws, then the OCR will either impose a fine upon the hospital\textsuperscript{51} or reach a settlement agreement with the hospital.\textsuperscript{52} If the OCR assesses penalties against the covered entity, then the covered entity pays that fine to the federal government rather than the individual victims of the cyberattack.\textsuperscript{53} As a result, an individual person will not recover any monetary damages at the

\begin{itemize}
\item \textsuperscript{43} Id.
\item \textsuperscript{44} Id. § 17932(e)(2)-(4).
\item \textsuperscript{45} See McMahon, supra note 12, at 644.
\item \textsuperscript{46} See Mark A. Hall et al., Health Care Law and Ethics 170 (8th ed. 2013).
\item \textsuperscript{47} Id. at 172.
\item \textsuperscript{48} EZOR, supra note 20, at 167.
\item \textsuperscript{50} See 45 C.F.R. § 160.306(a); see also OCR, HIPAA What to Expect, supra note 49.
\item \textsuperscript{51} See 45 C.F.R. § 160.402; see also OCR, HIPAA What to Expect, supra note 49.
\item \textsuperscript{52} See 45 C.F.R. § 160.416; see also OCR, HIPAA What to Expect, supra note 49.
\item \textsuperscript{53} See 45 C.F.R. § 160.424.
\end{itemize}
conclusion of an OCR investigation.\textsuperscript{54} Instead, that individual must resort to tort and contract remedies in state and federal courts for legal redress.\textsuperscript{55}

Additionally, personal health records created and stored on medical devices and third-party applications are not included within HIPAA’s regulatory framework because these applications are not considered “covered entities” for HIPAA purposes.\textsuperscript{56} Because these medical devices and applications are neither “covered entities” nor “business associates,” HIPAA does not protect the valuable medical information stored on these devices and within these applications.\textsuperscript{57}

For example, many Americans rely on medical devices such as pacemakers or glucose meters to track and store their medical data.\textsuperscript{58} Oftentimes, these devices do not fall under the HIPAA Rules; instead, the Food and Drug Administration promulgates the appropriate security regulations.\textsuperscript{59} Health tracking applications such as Fitbit, MyFitness Pal, or Apple Health have also become increasingly popular.\textsuperscript{60} Interestingly, the default settings on an Apple Watch automatically monitor the user’s activity, including heart rate and the number of steps taken throughout the day.\textsuperscript{61} Apple Watch and iPhone users can also monitor their calorie intake, the number of minutes spent meditating, and the number of hours spent sleeping on Apple’s Health application.\textsuperscript{62} Commentators have expressed concern that “HIPAA and other federal and state privacy laws are too focused on formal data custodians and data collected in narrow contexts of treatment and medical research.”\textsuperscript{63} As a result, there is an entire swath of patient medical information that is unprotected by HIPAA; this valuable medical data is even more vulnerable to a cyberattack than the medical data stored by a hospital.\textsuperscript{64}

\begin{flushleft}
54. See EZOR, supra note 20, at 167 (explaining that private litigation is one way for a victim of a hospital cyberattack to seek recovery).
55. See id.
57. Id.
59. Id. at 107-08.
60. See Cohen & Mello, supra note 56, at 232.
61. Use the Health App on Your iPhone or iPod Touch, APPLE (Nov. 29, 2018), https://support.apple.com/en-us/HT203037.
62. Id.
64. Id.
\end{flushleft}
HITECH laws, hospitals have also become increasingly prone to cyberattacks in the past decade.\footnote{Lucy L. Thomson, *Health Care Data Breaches and Information Security*, in *Health Care IT* 253, 253 (Arthur Peabody, Jr. ed., 2013).}

**D. Recent Cyberattacks at Large Hospitals in the United States**

The need for further legislation is made clear by the increased likelihood of cyberattacks upon the health-care industry. According to a report from the FBI Cyber Division, electronic medical records can be sold on the black market for up to $50 per record.\footnote{FBI Cyber Div., *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (2014), http://www.calhospital.org/sites/main/files/file-attachments/dp_attachment_fbi_alert.pdf.} In comparison, stolen social security numbers or credit card numbers are only worth $1 on the black market.\footnote{Id.} Like financial records, medical records often contain a patient’s social security number and credit card numbers.\footnote{Id.} As a result, electronic health data is often more valuable to hackers than financial records alone.\footnote{Id.}

In addition to credit card and social security numbers, electronic medical records also contain valuable information about a patient’s health insurance.\footnote{Id.} This data is extremely valuable to hackers because it can be used to buy medical equipment or prescription drugs.\footnote{Id.} Because doctors and nurses rely so heavily upon the information within the patient’s medical record to treat the patient, medical identity theft raises serious concerns about the integrity of the data in the medical record.\footnote{See Scott Rupp, *Why Do Hackers Want Medical Records?*, *Electronic Health Rep.* (Apr. 18, 2018), https://electronichealthreporter.com/hackers-want-medical-records/.} A stolen medical identity can pose a serious health risk if an unconscious patient has been rushed to the emergency room and cannot verify his or her past medical or prescription history.\footnote{Id.} Because the patient cannot speak, the doctors and nurses must instead rely upon the medical information within the patient’s chart.\footnote{See id.} If the information in that patient’s chart has been corrupted due to medical identity theft, this creates

---

\begin{footnotes}
\item[67.] Id.
\item[69.] Id.
\item[70.] Id.
\item[71.] Id.
\item[73.] Id.
\item[74.] See id.
\end{footnotes}
the dangerous possibility that a doctor or nurse could accidently administer a dangerous dose of medication or begin a transfusion using the wrong blood type.\textsuperscript{75}

To further exacerbate the problem, the United States health-care system is notoriously vulnerable due to legacy equipment and limited information technology budgets; thus, hospitals and health insurance providers are easy targets for cyberattacks.\textsuperscript{76} Additionally, HIPAA and the HITECH Act have created incentives for hospitals to install electronic medical record software, and the recent “efforts to modernize healthcare facilities to match the rapidly advancing technological landscape has created and exposed a host of vulnerabilities that are actively targeted by malicious parties.”\textsuperscript{77} These additional vulnerabilities can be expected because “[o]ften, technology is involved in various privacy problems, as it facilitates the gathering, processing, and dissemination of information.”\textsuperscript{78} A hospital’s electronic medical records are no different: “[m]assive data storage can also be vulnerable to cyberattacks and inadvertent release of sensitive data.”\textsuperscript{79} In describing the issues related to cyberattacks at hospital systems, the Health Care Industry Cybersecurity Task Force, which was created by Congress as a part of the Cybersecurity Act of 2015, states unequivocally: “cybersecurity attacks disrupt patient care.”\textsuperscript{80}

As a result, patient medical data has been particularly vulnerable to cyberattacks.\textsuperscript{81} In 2018, nearly ten million medical records were compromised.\textsuperscript{82} 2015 was a record year for compromised health records; over 121 million health-care records were compromised.\textsuperscript{83} Since 2014, hackers have gained access to 161,080,500 health-care records.\textsuperscript{84}

\textsuperscript{75} See id.
\textsuperscript{76} See Health Care Indus. Cybersecurity Task Force, supra note 1, at 1.
\textsuperscript{79} Gostin et al., supra note 63, at 234.
\textsuperscript{80} Health Care Indus. Cybersecurity Task Force, supra note 1, at 1.
\textsuperscript{81} Id.
Even outside of the health-care space, data breaches are important matters of public concern. The 2017 Equifax data breach exposed the private financial information of at least 148 million Americans. The attack affected nearly 45% of American consumers, those consumers must now actively monitor their credit reports for decades in order to protect against identity theft. This massive data breach received broad media coverage and increased public awareness about the vulnerability of our private data as well as the need for additional data security.

Following the Equifax data breach, hospital data breaches should start receiving greater national attention. Americans would be surprised to learn that over 161 million patient health records have been compromised since 2014. This number is greater than the number of records stolen in the Equifax data breach. Hospital data breaches are a serious and systemic problem that should be receiving the same national media attention as the 2017 Equifax hack.

The 2015 data breach of the nation's largest health insurance provider, Anthem Inc. (Anthem), reveals the dramatic threat of cyberattacks on our nation's hospitals and health insurance providers. Cyber criminals hacked into Anthem's network and stole the medical records of over 79 million patients.

In the aftermath of the Anthem hack, both the OCR and private plaintiffs pursued claims against Anthem; the OCR investigated the cyber breach, and consumers sought damages in a class action.

---

85. EQUIFAX ONE YEAR LATER—AFTERMATH REPORT, supra note 4, at 1.
86. See id.
88. See id. at 552-53.
89. See 2018 END-OF-YEAR DATA BREACH REPORT, supra note 82; 2016 END OF YEAR REPORT, supra note 84; 2015 DATA BREACH REPORTS, supra note 83; 2014 DATA BREACH REPORTS, supra note 84.
90. EQUIFAX ONE YEAR LATER—AFTERMATH REPORT, supra note 4, at 1.
lawsuit in federal court.\textsuperscript{94} The Anthem case was the largest health-care data breach in history, and consequently, its $16 million settlement with HHS and the OCR was the largest HIPAA settlement ever reached.\textsuperscript{95} The victims of the Anthem attack will not receive this money; instead, the settlement will be paid to the United States Treasury.\textsuperscript{96}

In the civil suit, Anthem and the class-action plaintiffs reached a civil settlement of $115 million.\textsuperscript{97} When divided among the class members, that settlement can only compensate the victims for two years of credit monitoring services.\textsuperscript{98} If the class members had already enrolled with a credit monitoring service, then those plaintiffs may be eligible to receive a $50 cash payment.\textsuperscript{99} Despite obtaining one of the largest data breach settlements in history, it is clear that neither a $50 payment nor two years of free credit monitoring services can adequately compensate the victims for this egregious disclosure of their most private data.\textsuperscript{100} In fact, this pitiable compensation is typical of the settlement awards received by data breach victims.\textsuperscript{101} For example, the Equifax data breach victims received a similar settlement for one year of credit monitoring.\textsuperscript{102}

Oftentimes, the victims of medical identity theft must take steps to resolve the identity theft on their own initiative.\textsuperscript{103} The resolution of a cyberattack can be both costly and time consuming.\textsuperscript{104} Thirty six percent of the victims of a cyberattack spent an average of $18,660 to resolve the identity theft.\textsuperscript{105} These expenses include the cost of identity protection, credit reporting, legal counsel, medical services due to a lapse of health-care coverage, and reimbursements to health-care providers to pay for the medical expenses incurred by imposters.\textsuperscript{106} Additionally, the resolution of a cybercrime can be extremely time consuming.\textsuperscript{107} In fact, many patients report

\textsuperscript{94} Anthem, supra note 91.
\textsuperscript{95} Teichert, supra note 93.
\textsuperscript{96} See 45 C.F.R. § 160.424 (2019).
\textsuperscript{97} Teichert, supra note 93.
\textsuperscript{98} Id.
\textsuperscript{99} Anthem, supra note 91.
\textsuperscript{100} See Teichert, supra note 93.
\textsuperscript{101} See Smith & Mulrain, supra note 87, at 556.
\textsuperscript{102} See id. (noting that "the one-year protection plan fell far short of what was needed for aggrieved customers").
\textsuperscript{104} Id.
\textsuperscript{105} Id. at 4-5.
\textsuperscript{106} Id.
\textsuperscript{107} Id. at 2.
that it has taken a year or longer to resolve their case of medical identity theft.\footnote{Id.}

\subsection*{E. Why We Need Additional Protection over Our Electronic Medical Records}

Because of the increased threat of cyberattacks, the courts and legislatures must proactively respond to this impending threat.\footnote{Edelson & Lawson, supra note 7, at 106.} The recent Anthem data breach “should be a call to arms” for all hospitals and health insurance providers.\footnote{Id.} Despite the severity of the situation, “[s]ignificant players in the healthcare space, however, have not responded to these incidents with the urgency that, we believe, the situation requires. They are instead content to cast themselves as unwitting victims, even when best practices dictate more proactive measures.”\footnote{Id.}

Because electronic medical records contain a person’s most private data, we must work proactively to improve our hospital cybersecurity.\footnote{Id.} The Health Care Industry Cybersecurity Task Force, which was created by Congress as a part of the Cybersecurity Act of 2015, explains that although a one-year identity protection plan is standard across other industries following a cyberattack, this solution is insufficient in the health-care space because “it does not provide the patient with adequate protections based on the sensitivity, value, and permanence of their health care data, which is priceless.”\footnote{Thomson, supra note 65, at 264.}

Electronic patient medical information is more valuable to hackers than basic financial information alone.\footnote{FBI CYBER DIV., supra note 66.} Electronic medical records typically contain a patient’s social security number as well as credit card or banking information.\footnote{Sweeney, supra note 68.} These records, however, also contain the most private and intimate details about that person’s life.\footnote{Thomson, supra note 65, at 264.} They can contain details about patients’ sexually transmitted diseases, pregnancies, mental health records, and drug histories.\footnote{Id.} Some of this information may be embarrassing and could

\begin{itemize}
  \item \footnote{Id.}
  \item \footnote{Edelson & Lawson, supra note 7, at 106.}
  \item \footnote{Id.}
  \item \footnote{Id.}
  \item \footnote{Thomson, supra note 65, at 264.}
  \item \footnote{Health Care Indus. Cybersecurity Task Force, supra note 1, at 15 (emphasis added).}
  \item \footnote{FBI CYBER DIV., supra note 66.}
  \item \footnote{Sweeney, supra note 68.}
  \item \footnote{Thomson, supra note 65, at 264.}
  \item \footnote{Id.}
\end{itemize}
even be used to unlawfully discriminate against individuals in the workplace.\footnote{118}

For example, a railroad company was fined by the Equal Employment Opportunity Commission for secretly conducting genetic testing upon its employees to screen for diseases that could negatively affect job performance.\footnote{119} This example illustrates how an electronic medical record could potentially contain personal genetic information that could be used to discriminate against the patient in the workplace. Furthermore, researchers increasingly use biobanks storing “large sets of patient data and biological samples” in attempts to understand and cure diseases.\footnote{120} Advances in biobank research, however, create confidentiality and privacy concerns if the information in the biobank has not been properly de-identified.\footnote{121} The genetic material stored in a biobank is literally the essence of that individual person.\footnote{122} As a result, we must make every effort to protect this personal health information.

III. ANALYSIS

The law must intervene to help protect patients from the increased threat of cyberattacks upon our electronic medical records. This article proposes both a judicial and legislative solution to help address the indignity that occurs when cyber criminals access and steal a patient’s valuable medical data. This author proposes a judicial and legislative solution to help combat the increased problem of hospital cyberattacks. First, this author proposes that the United States Supreme Court recognize a fundamental right to the privacy of our medical records based upon prior Supreme Court decisions regarding information privacy and medical decision making. Additionally, this article proposes that the OCR should modify all “addressable” standards within the HIPAA Security Rules to be “required” for all large covered entities.\footnote{123}

\footnotesize
\begin{enumerate}
\item[118.] EZOR, supra note 20, at 102.
\item[120.] HALL ET AL., supra note 46, at 276.
\item[122.] See Catherine M. Valerio Barrad, Comment, Genetic Information and Property Theory, 87 Nw. L. Rev. 1037, 1071 (1993) (“A person’s DNA existed from the moment he began to exist as an individual. In addition, the individual has no control over the specific information encoded in his DNA that determines his unique characteristics or traits; this information also existed intact at the time the person began to exist.”).
\item[123.] 45 C.F.R. § 164.306(b)-(d) (2019).
\end{enumerate}
A. Proposed Judicial Solution: Affording Federal Constitutional Protection to Patient Medical Records

As the threat of cyberattacks increases, HIPAA laws no longer adequately protect our patient health information. Additionally, state and federal governments have increasingly begun to accumulate and store both identified and de-identified health information for reporting and research purposes. Of the 6,210 hospitals in the United States, 1,180 of those hospitals are public hospitals that are operated by either state or federal governments. Thus, government entities have increasingly begun to aggregate, collect, and store our electronic medical data.

Some patients could turn to the United States Constitution to help protect their private medical records. This article proposes the creation of a fundamental right to the privacy of our medical records. This proposed fundamental privacy right is derived from previous Supreme Court decisions discussing information privacy and medical privacy, as well as the common-law doctrines of implied breach of contract, assault, and battery. A fundamental privacy right to medical records would afford patients the security of knowing that their medical records and, ultimately, their medical decisions are protected under the Constitution.

---

124. HEALTH CARE INDUS. CYBERSECURITY TASK FORCE, supra note 1, at 1.
127. Mariner, supra note 125, at 976.
131. See generally Whalen, 429 U.S. at 600, 605 (noting the "genuine concern" that private health data may be inadvertently released when "vast amounts of personal information" is stored "in computerized data banks or other massive government files").
1. A Constitutional Right to Informational Privacy

Based upon the constitutional right to information privacy discussed in Whalen v. Roe\textsuperscript{132} and NASA v. Nelson,\textsuperscript{133} the Supreme Court should recognize the existence of a constitutional right to information privacy. This constitutional right to information privacy should also protect the privacy of our electronic medical records. In Whalen v. Roe, the United States Supreme Court first recognized that a constitutional right to information privacy may exist.\textsuperscript{134} The plaintiffs in this case challenged a New York state law that created a database that stored the names and addresses of all patients using Schedule II drugs for both medical and nonmedical purposes.\textsuperscript{135} The plaintiffs alleged that the storage of their personal medical information within the database violated their constitutional privacy rights.\textsuperscript{136} The Court held that the right to privacy protects at least two different interests: the right to avoid disclosure of personal matters and a right to independence in decision making.\textsuperscript{137} The Court further recognized that the storage of this medical information in the state database presents

\begin{quote}
  a genuine concern that the information will become publicly known and that it will adversely affect their reputations. This concern makes some patients reluctant to use, and some doctors reluctant to prescribe, such drugs even when their use is medically indicated. It follows, they argue, that the making of decisions about matters vital to the care of their health is inevitably affected by the statute. Thus, the statute threatens to impair both their interest in the nondisclosure of private information and their interest in making important decisions independently.\textsuperscript{138}
\end{quote}

Because the state had provided adequate protections over the information stored in the database, the Court ultimately held that this database was constitutional.\textsuperscript{139} The Court acknowledged, however, that it was “not unaware of the threat of privacy implicit in

\begin{itemize}
  \item \textsuperscript{132} 429 U.S. at 605.
  \item \textsuperscript{133} 562 U.S. at 138.
  \item \textsuperscript{134} 429 U.S. at 591-93.
  \item \textsuperscript{135} Id. at 591.
  \item \textsuperscript{136} Id. at 599-600.
  \item \textsuperscript{137} Id.
  \item \textsuperscript{138} Id. at 600.
  \item \textsuperscript{139} Id. at 603-04.
\end{itemize}
the accumulation of vast amounts of personal information in computerized data banks or other massive government files.”¹⁴⁰ And the right of a government entity “to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.”¹⁴¹ Additionally, the Court acknowledged that this duty to avoid the unwarranted disclosure of the plaintiffs’ private medical information “arguably ha[d] its roots in the Constitution.”¹⁴² Although the Court did not ultimately create a constitutional duty mandating that government entities must protect the privacy of the electronic information within their possession, it certainly suggested that such a duty could exist.¹⁴³ The lower federal courts have since read Whalen to create a duty to safeguard the private information that is entrusted to government entities.¹⁴⁴

The Supreme Court further hinted that this right to information privacy may exist in NASA v. Nelson.¹⁴⁵ In this case, National Aeronautics and Space Administration (NASA) employees claimed that the government violated their constitutional privacy interests in avoiding the wrongful disclosure of personal matters through the administration of NASA’s standard employee background investigation.¹⁴⁶ The challenged background investigation included questions about prior treatment for illegal drug use.¹⁴⁷ Writing for the majority, Justice Alito stated: “[w]e assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in Whalen.”¹⁴⁸ The Court observed that the “remote possibility” of disclosure of this private information “does not undermine the Privacy Act’s substantial protections.”¹⁴⁹ The Court ultimately held “that the Government’s inquiries do not violate a constitutional right to informational privacy.”¹⁵⁰ In a concurring opinion, Justice Scalia wrote separately to clarify that “[a] federal constitutional right to ‘informational privacy’ does not exist.”¹⁵¹ Based upon the holdings in Whalen v. Roe and NASA v. Nelson, courts should recognize the

¹⁴⁰. Id. at 605.
¹⁴¹. Id.
¹⁴². Id.
¹⁴³. Id.
¹⁴⁴. Solove, supra note 78, at 518, 530.
¹⁴⁶. Id.
¹⁴⁷. Id.
¹⁴⁸. Id.
¹⁴⁹. Id. at 158.
¹⁵⁰. Id. at 159.
¹⁵¹. Id. at 160 (Scalia, J., concurring).
right to information privacy and should include the privacy of our electronic medical information within that constitutional right.

2. A Constitutional Right to Dignity in Medical Decision Making

Whalen v. Roe\textsuperscript{152} and NASA v. Nelson\textsuperscript{153} support the argument that a constitutional right to information privacy should exist,\textsuperscript{154} and furthermore, the Supreme Court decisions in Cruzan v. Director, Missouri Department of Health\textsuperscript{155} and Washington v. Glucksberg\textsuperscript{156} suggest that the Constitution protects the right to freedom in our health-care decisions.\textsuperscript{157} In Cruzan, the Supreme Court recognized that a patient possesses a fundamental privacy right to terminate medical treatment at the end of life.\textsuperscript{158} In this case, the Court considered whether the parents of an incompetent young woman living in a persistent vegetative state could make the decision to terminate their daughter’s life support.\textsuperscript{159} The challenged Missouri state law required a heightened showing of an incompetent person’s wishes whenever a surrogate makes the decision to terminate life support on an incompetent person’s behalf.\textsuperscript{160} Although the Court ultimately found that the patient’s as applied challenge must fail, the Court included statements about the individual right to autonomy in medical decision making.\textsuperscript{161} The majority opinion, written by Chief Justice Rehnquist, stated, “we assume that the United States Constitution would grant a competent person a constitutionally protected right to refuse lifesaving hydration and nutrition.”\textsuperscript{162} Justice O’Connor wrote a concurring opinion where she clarified that:

[r]quiring a competent adult to endure such procedures against her will burdens the patient’s liberty, dignity, and freedom to determine the course of her own treatment. Accordingly, the liberty guaranteed by the Due Process Clause must protect, if it protects anything, an individual’s deeply personal

\begin{itemize}
\item[152.] 429 U.S. 589, 605 (1977).
\item[153.] 562 U.S. at 138.
\item[154.] Id.; Whalen, 429 U.S. at 605.
\item[156.] 521 U.S. 702, 725 (1997).
\item[157.] Id.; Cruzan, 497 U.S. at 279.
\item[158.] Cruzan, 497 U.S. at 279.
\item[159.] Id. at 265.
\item[160.] Id. at 268-69.
\item[161.] Id. at 273.
\item[162.] Id.
\end{itemize}
decision to reject medical treatment, including the artificial delivery of food and water.\textsuperscript{163}

Justice Brennan’s dissent discussed the importance of dignity in medical decision making.\textsuperscript{164} Justice Brennan described the decision of whether to continue medical treatment at the end of life as both “difficult and personal.”\textsuperscript{165} Justice Brennan explained “that [the young woman] has a fundamental right to be free of unwanted artificial nutrition and hydration,” and, as a result, she “is entitled to choose to die with dignity.”\textsuperscript{166} Thus, he would have found that the challenged Missouri law could not pass the strict scrutiny test.\textsuperscript{167}

In the landmark physician-assisted suicide case of Washington \textit{v. Glucksberg}, the Court considered “how best to protect dignity and independence at the end of life.”\textsuperscript{168} In fact, in her concurrence, Justice O’Connor advocated for what is known as the principle of double effect: “a patient who is suffering from a terminal illness and who is experiencing great pain has no legal barriers to obtaining medication, from qualified physicians, to alleviate that suffering, even to the point of causing unconsciousness and hastening death.”\textsuperscript{169} Justice Stevens concurred in the judgment and explained that the right to refuse medical treatment at the end of life “is an aspect of a far broader and more basic concept of freedom that is even older than the common law. This freedom embraces not merely a person’s right to refuse a particular kind of unwanted treatment, but also her interest in dignity . . . .”\textsuperscript{170}

The \textit{Cruzan} and \textit{Glucksberg} decisions support the argument that the Constitution protects our freedom and individual liberty in decision making regarding our personal health-care choices. This freedom in medical decision making includes the decision of whom we choose to share our most confidential medical information with. A hospital breaks patient confidentiality whenever its data is breached. Whenever a hospital data breach occurs, a hospital thus breaks patient confidentiality. The hospital data breach is a violation of the patient’s personal liberty because that patient no longer controls who has access to his or her medical information. Thus, a

\textsuperscript{163} Id. at 289 (O’Connor, J., concurring).
\textsuperscript{164} See id. at 302 (Brennan, J., concurring).
\textsuperscript{165} Id. at 303.
\textsuperscript{166} Id. at 302.
\textsuperscript{167} Id.
\textsuperscript{168} 521 U.S. 702, 716 (1997).
\textsuperscript{169} Id. at 736-37 (O’Connor, J., concurring).
\textsuperscript{170} Id. at 743 (Stevens, J., concurring).
data breach violates the constitutional principle of freedom in medical decision making established in *Cruzan* and *Glucksberg* because it takes away the patient’s choice of deciding who gets to learn about his or her most private health information.

3. *A Constitutional Right to the Privacy of Our Patient Medical Records*

Although many of the Justices spoke of human dignity and individual privacy rights in the *Cruzan* and *Glucksberg* opinions, *Cruzan* recognized, as a facet of those privacy rights, a “constitutionally protected liberty interest in refusing unwanted medical treatment.”171 This liberty interest is based upon the common-law doctrine of informed consent.172 The Court explained that “[a]t common law, even the touching of one person by another without consent and without legal justification was a battery.”173 As a part of this common-law “notion of bodily integrity,”174 the patient has a right “not to consent, that is, to refuse treatment.”175

Conversely, the *Glucksberg* Court held that a patient does not have a fundamental privacy right to a physician-assisted suicide.176 The *Glucksberg* Court performed a historical analysis and determined that the law has never recognized a common-law right to commit suicide or to assist another person in committing suicide.177 The Court noted that “for over 700 years, the Anglo-American common-law tradition has punished or otherwise disapproved of both suicide and assisting suicide.”178 As a result, the Court declined to recognize an individual privacy right to physician-assisted suicide.179

Writing for the majority in *Glucksberg*, Chief Justice Rehnquist distinguished the *Cruzan* case from the matter before the Court, explaining that “[t]he right assumed in *Cruzan*, however, was not simply deduced from abstract concepts of personal autonomy.”180 Instead, the fundamental right recognized in *Cruzan* was based upon “the common-law rule that forced medication was a battery,

---

171. *Cruzan*, 497 U.S. at 278.
172. *Id.* at 269-70.
173. *Id.* at 269.
174. *Id.*
175. *Id.* at 270.
177. *Id.* at 710-16.
178. *Id.* at 711.
179. *Id.* at 735.
180. *Id.* at 725.
and the long legal tradition protecting the decision to refuse unwanted medical treatment, our assumption was entirely consistent with this Nation’s history and constitutional traditions.” 181 The Court acknowledged that “[t]he decision to commit suicide with the assistance of another may be just as personal and profound as the decision to refuse unwanted medical treatment, but it has never enjoyed similar legal protection.” 182

The courts should recognize that the Constitution protects a fundamental right to the privacy of our patient medical records. Although the common-law privacy right is a relatively new development in the history of the common law, courts can rely on the more ancient doctrines of implied breach of contract, assault, and battery as the source of this fundamental right. 183 By relying upon these well-established common-law doctrines, the fundamental right to privacy of our medical records is thus rooted in “this Nation’s history and constitutional traditions.” 184

The common-law privacy right, which is distinct from the constitutional privacy right recognized in Griswold v. Connecticut, 185 Roe v. Wade, 186 Cruzan v. Director, and Missouri Department of Health, 187 was first discerned in the classic Harvard Law Review article written by Samuel Warren and Louis Brandeis, The Right to Privacy. 188 Warren and Brandeis argued that the advances of modern technology during the industrial age created the necessity for a common-law privacy right. 189 Warren and Brandeis examined a variety of common-law cases and perceived that the right to privacy existed within the common-law doctrines of assault and battery, 190 property law, 191 slander, 192 libel, 193 breach of an implied contractual term, 194 and breach of confidence. 195

181. Id.
182. Id.
183. See generally Warren & Brandeis, supra note 130, at 193-94, 210-11 (explaining how the common-law doctrines of breach of contract, assault, and battery lead to the creation of a tort cause of action for breach of privacy).
184. Glucksberg, 521 U.S. at 725.
188. Warren & Brandeis, supra note 130, at 213.
189. Id. at 195-96.
190. Id. at 193-94.
191. Id. at 204.
192. Id. at 197.
193. Id.
194. Id. at 210-11.
195. Id. at 207-08.
Following the publication of *The Right to Privacy* in 1890, the courts slowly began to recognize a cause of action based upon the invasion of privacy.\(^\text{196}\) The Restatement of Torts first recognized a tort cause of action for the interference with privacy in 1939.\(^\text{197}\) In 1960, Dean William Prosser revisited *The Right to Privacy* in his own famous law review article discussing the right to privacy.\(^\text{198}\) In this article, Dean Prosser examined the evolution of the common-law privacy right since the publication of *The Right to Privacy* in 1890.\(^\text{199}\) After examining hundreds of judicial decisions across the country, Dean Prosser concluded that the right to privacy had fully emerged as a common-law cause of action in the United States.\(^\text{200}\)

Although the common-law privacy doctrine may seem to be the most fitting common law analogy for the recognition of a fundamental right to the privacy of our medical records, the right of privacy is only a recent common law development;\(^\text{201}\) as a result, this common-law privacy right cannot be considered part of the history and traditions of our country. Instead, the courts must rely upon an even older common-law doctrine that is rooted in the history and traditions of our country to find a new fundamental right that protects the privacy of our medical records.\(^\text{202}\)

*The Right to Privacy* cited to the common-law doctrines of implied breach of contract, assault, and battery in support of its authors' newly proposed common-law privacy right.\(^\text{203}\) Today, courts can rely upon these same three common-law doctrine in support of a fundamental right to the privacy of our medical information.

Warren and Brandeis cited the common-law doctrine of implied contractual terms in support of their proposed privacy right.\(^\text{204}\) Similarly, the common-law doctrine of implied contractual terms can also be used to establish a new fundamental right to the privacy of our medical records. Enforcing the implied terms in a contract has been a feature of the common law since the time of the founding; in 1807, the United States Supreme Court defined an implied con-

---


\(^{197}\) Restatement of Torts § 867 (Am. Law Inst. 1939).

\(^{198}\) Prosser, supra note 196, at 383-88.

\(^{199}\) Id.

\(^{200}\) Id. at 422.

\(^{201}\) See id. at 383-388 (describing how the courts slowly began to recognize a privacy cause of action in tort law following the publication of *The Right to Privacy* in 1890).

\(^{202}\) See Washington v. Glucksberg, 521 U.S. 702, 710 (1997) (noting that the Court begins its inquiry, "as we do in all due process cases, by examining our Nation's history, legal traditions, and practices").

\(^{203}\) Warren & Brandeis, supra note 130, at 193-94, 210-11.

\(^{204}\) Id. at 210-11.
tract as "that which the law (to prevent a failure of justice) presumes the parties to have made, where they have failed to make an express contract for themselves; and courts will vary the terms of such implied contract according to the principles of natural justice." 205  Contract law is a particularly appropriate analogy in the context of medical records because recent scholars have explained that the law of contracts is necessary to understand the relationship between a doctor and a patient.206  The doctor-patient relationship "is contractual in two important ways: it is a voluntary relationship and once initiated, it is subject to the application of principles from the law of contracts in the determination of the rights and duties of the parties." 207

Although the common law may not have recognized a cause of action for the breach of confidentiality in an individual doctor-patient relationship at the time of the founding,208 the large-scale collection, aggregation, and storage of electronic medical records in modern times presents a unique set of challenges that did not exist before the invention of computers. Because federal laws heavily incentivize and encourage the use of electronic medical records, patients have no choice but to accept that their patient information will be stored electronically by large hospital systems.209 Because patients have no control over hospital cyber-security measures, patients also must accept that their electronic medical information may be vulnerable to cyberattacks. As a result, patients have no choice but to trust that their hospitals will keep their private information safe from a data breach.

Because of the disproportionate relationship between the patient and the hospital, courts should recognize that an implied term exists within this contractual relationship. That implied term would include a promise from the hospital to protect the patient's medical records from a cyberattack. Hospital systems would thus break that implied promise every time that a patient's confidential medical record has been compromised in a data breach.

207. Id.
The modern-day contract between the hospital system and the patient is of greater financial significance than the contract between a local doctor and a patient at the time of the founding. That original relationship was based upon trust and personal interactions, whereas the medical system today has been described as “more impersonal and less humane.”

Interestingly, some authors argue that the introduction of health information technology, including electronic medical records software, is partially responsible for the “depersonalization of health care.” Because the practice of medicine has changed significantly since 1791, courts should recognize the existence of an implied contract term to secure all patient health records within the context of the modern-day doctor-patient relationship.

Warren and Brandeis also relied upon the evolution of the law of assault and battery in support of their newly proposed privacy right. The Right to Privacy discussed how the common-law doctrine of battery, which was designed to protect a person from physical injury, subsequently led to the creation of assault law. Assault law evolved from the law of battery under the theory that assault law protected an individual from the threat of a physical injury rather than the actual physical injury itself. The authors thus argued that assault law had led to the inevitable creation of “the right to be let alone” and their newly proposed privacy right.

Similarly, the cyberattacks upon our electronic medical records can be compared to the common-law doctrines of assault and battery. Warren and Brandeis explained in The Right to Privacy that battery and assault law evolved to protect every individual’s right to bodily integrity. Although electronic medical records are certainly intangible records, these records contain some of the most intimate details about a person’s tangible, physical body. If the law is prepared to accept assault and battery as an affront to our physical personhood, then the common-law concepts of assault and battery should also apply to our electronic personhood. With the recent scientific breakthroughs in genetic testing, biobanks, and
gene therapy, our electronic medical records contain more detailed intangible information about our tangible, physical bodies. As a result, a cyberattack upon a hospital system is more than a simple data breach. It is a digital assault upon our electronic personhood. Thus, courts can analogize to the ancient common-law doctrines of assault and battery to establish a new fundamental right to the privacy of our medical records.

In addition to federal constitutional protection, patients can also look to the constitutions of their respective states for additional protection over their electronic medical records. Each individual state has its own state constitution that can provide greater protections for individual liberties than the federal Constitution alone. The federal Constitution is a floor not a ceiling. And state constitutions may provide greater individual rights than the federal Constitution. In his often-quoted law review article discussing the power of the state constitutions, Justice Brennan opined “[s]tate constitutions, too, are a font of individual liberties, their protections often extending beyond those required by the Supreme Court’s interpretation of federal law.” As a result, absent precedent from the United States Supreme Court creating a fundamental right to the privacy of our electronic medical records, the state supreme courts can intervene and decide that patients have a fundamental right to the protection of their electronic medical records. State courts may be even more eager to create this new fundamental privacy right if the citizens of that particular state have been especially victimized by large-scale data breaches.

B. Proposed Legislative Solution: Making All Addressable HIPAA Standards Required for Large Covered Entities

Congress and the OCR can also protect the privacy of our medical records through the implementation of legislative reform. Because of the devastating consequences of a medical data breach, Congress and HHS should adopt additional regulations to help monitor and

\[218. \text{Id.} \]
\[219. \text{ROBERT F. WILLIAMS, THE LAW OF AMERICAN STATE CONSTITUTIONS 114 (2009).} \]
\[221. \text{Id.} \]
\[222. \text{William J. Brennan, Jr., State Constitutions and the Protection of Individual Rights, 90 HARV. L. REV. 489, 491 (1977).} \]
\[223. \text{See supra notes 219-222 and accompanying text.} \]
prevent cyberattacks. Congress and HHS must create stronger protections of our valuable patient health data through federal legislation.\footnote{224 See, e.g., Solove, supra note 78, at 564 (explaining that “[t]he way to address privacy problems is to regulate these activities”); Edelson & Lawson, supra note 7, at 106 (urging that the inaction of hospitals and health insurance providers to take proactive measures to prevent data breaches “requires legislators and the courts to intervene before it is too late”); HEALTH CARE INDUS. CYBERSECURITY TASK FORCE, supra note 1, at 2 (noting that “health care cyber security is a key public health concern that needs immediate and aggressive attention”).}

Currently, the HIPAA Privacy and Security Rules permit a degree of flexibility for covered entities; however, HHS should ensure that large covered entities adopt even stricter security standards.\footnote{225 See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH and GINA Acts, 78 Fed. Reg. 5566, 5589 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164) (noting that “the requirements of the Security Rule were designed to be technology neutral and scalable to all different sizes of covered entities and business associates); see also JOHN J. TRINCKES, JR., THE DEFINITIVE GUIDE TO COMPLYING WITH THE HIPAA/HITECH PRIVACY AND SECURITY RULES 167 (2013) (explaining that “the HIPAA Security Rule is designed to be scalable across small and large covered entities”).}

This article proposes that all “addressable” standards in the HIPAA Security Rule should be “required” standards for all large covered entities. This solution will also include a provision that allows smaller independent doctor’s offices to continue to make case-by-case determinations of whether to implement HIPAA’s addressable standards.\footnote{226 45 C.F.R. § 164.306(b)-(d) (2019).}

Many other authors have offered suggestions and ideas for reforming hospital cyber security. These solutions have ranged from monumental changes, such as large scale privacy reform in the United States modeled after the European Union’s General Data Protection Regulation,\footnote{227 Elizabeth A. Brasher, Note, Addressing the Failure of Anonymization: Guidance from the European Union’s General Data Protection Regulation, 2018 COLUM. BUS. L. REV. 208, 251-53 (2018).} to incremental changes, such as requiring encryption of all health-care data.\footnote{228 Ryan L. Garner, Note, Evaluating Solutions to Cyber Attack Breaches of Health Data: How Enacting a Private Right of Action for Breach Victims Would Lower Costs, 14 IND. HEALTH L. REV. 127, 164 (2017).}

Student author, Ryan Garner, has recognized that the lack of data encryption at American hospitals poses a major threat to cyber security.\footnote{229 Id.} He offered a solution to amend the HIPAA Security Rule to change data encryption from an “addressable” standard to a “required” standard.\footnote{230 Id.} In fact, Garner’s suggestion helped to spark this author’s proposal. This paper builds upon Garner’s understanding of the need for additional security measures in order to
appropriately protect our nation’s electronic medical records.\textsuperscript{231} This paper also builds upon Garner’s recognition that the current version of HIPAA does not adequately protect our electronic medical records, and one way to address that deficiency is to build upon HIPAA’s existing framework to create additional cyber-security protections.\textsuperscript{232}

Readers may be surprised to learn that HIPAA actually offers some degree of flexibility for the enforcement of the HIPAA standards: although many of the standards found in the HIPAA Security Rules are “required,” some of the standards are “addressable.”\textsuperscript{233} If a standard is “addressable” rather than “required,” the covered entity may take the following factors into account when deciding whether to implement the security standard: “(i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity’s or the business associate’s technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.”\textsuperscript{234} This flexibility leads to a troubling result because it gives individual entities the ability to decide whether to adopt certain provisions of HIPAA’s Security and Privacy Rules.\textsuperscript{235} Currently, all covered entities are permitted to make a case-by-case determination over whether to implement the addressable HIPAA standards.\textsuperscript{236}

HIPAA would offer stronger cyber-security protections if HHS amended all the “addressable” security standards to now be “required” standards for all large covered entities.\textsuperscript{237} HHS considered, debated, and approved the addressable and required security standards when it initially promulgated HIPAA’s Security Rule in 2000.\textsuperscript{238} Professor Glenn Cohen of Harvard Law School and Professor Michelle Mello of Stanford Law School explain that despite the initial criticisms of HIPAA as being both too unwieldy and too narrow:

\begin{itemize}
  \item \textsuperscript{231} Id.
  \item \textsuperscript{232} Id.
  \item \textsuperscript{233} 45 C.F.R. § 164.306(d) (2019).
  \item \textsuperscript{234} Id. § 164.306(b)(2).
  \item \textsuperscript{235} TRINCKES, supra note 225, at 166-67.
  \item \textsuperscript{236} Id.
  \item \textsuperscript{237} 45 C.F.R. § 164.306(d)(1).
\end{itemize}
Over time, however, HIPAA has proved surprisingly functional. Particularly after being amended in the 2009 HITECH (ie, the Health Information Technology for Economic and Clinical Health) Act to address challenges arising from electronic health records, HIPAA has accomplished its primary objective: making patients feel safe giving their physicians and other treating clinicians sensitive information while permitting reasonable information flows for treatments, operations, research, and public health purposes.239

Because HIPAA already provides some protections over patient medical records, it will be a quicker and more efficient solution to build off the existing architecture of HIPAA and the HITECH Act rather than creating an entirely new framework for data privacy in the United States.

Although this relatively straightforward solution may not be as comprehensive as a massive overhaul of United States data privacy laws, it has the benefit of being more likely to occur. Because legislative reform takes time, a more moderate proposal may be the quickest way to affect actual change of hospitals and health insurance providers. This proposal does not preclude others from suggesting more impactful and lasting changes, but this solution has the benefit of offering a realistic short-term solution that will have a more immediate impact over the security of our electronic medical records.

This proposal also has the benefit of considering the size and resources of an individual provider or small physician group. One criticism of HIPAA is that “[t]he specifics are largely left to the provider and their capabilities and budget, which is the reason why there are such broad discrepancies in security across the healthcare industry.”240 When the OCR passed the HIPAA Security Rule, it understood that a one-size-fits-all solution would not work for every hospital and every health insurance provider in the country.241 In fact, “the HIPAA Security Rule is designed to be scalable across small and large covered entities. Since each covered entity is different, the rules were not developed to be so specific that a covered entity does not have the latitude to decide how best to meet the requirements.”242 Although it may have been desirable to leave some

239. Cohen & Mello, supra note 56, at 231.
240. Nguyen, supra note 77, at 105.
241. TRINCKES, supra note 225, at 167.
242. Id.
discretion up to the individual health-care providers when the Privacy and Security Rules were originally passed, the information age has left patients’ electronic medical records vulnerable to cyberattacks. The Equifax and Anthem data breaches prove that Congress can no longer depend upon the individual hospitals and health insurance providers to adequately protect the sensitive medical information that their patients have entrusted to them.

Under this proposal, changing the HIPAA standards from addressable to required will depend upon the entity’s size. HIPAA requirements already vary depending upon the covered entity’s size. This proposal is a continuation of that framework. This solution is both realistic and practical because it accomplishes the goal of creating greater protection over the electronic medical records at the large United States hospitals that hold the greatest proportion of patient data without imposing overly exacting monetary requirements upon smaller local practices. This solution follows the existing HIPAA framework by considering the varying resources and capabilities of health-care providers across the country. Small individual providers will not be forced to adopt the same degree of sophisticated technological infrastructure to protect against cybercrimes as a large health-care conglomerate. This solution considers that a small, independent doctor’s office has different constraints than a large covered entity such as Anthem, the largest health insurer in the country.

The increasing prevalence of cyberattacks on hospitals and health insurance companies is a serious threat to all American patients. The frequency and severity of these attacks has increased dramatically in recent years. The public backlash following the Equifax data breach demonstrates the public concern regarding the security of our personal data stored in the electronic files of our nation’s banks, hospitals, educational institutions, and government entities. Although other authors have called for more dramatic reform of data privacy laws in America, these proposals are outside of the scope of this article. Instead, this article proposes a modest solution to the immediate problem: cyber criminals compromise our electronic medical data on a daily basis. Although this proposal is modest, it is a first step towards assuring Americans that their

243. Id.
244. Anthem, supra note 91.
245. HEALTH CARE INDUS. CYBERSECURITY TASK FORCE, supra note 1, at 1.
246. Thomson, supra note 65, at 253.
medical records are properly safeguarded by the institutions that they are entrusting with the custody of their electronic medical records.

IV. CONCLUSION

The threat of a large-scale data breach of our electronic health records should be a serious concern for all Americans. The protected health information that is collected, stored, and aggregated at hospitals and health insurance providers nationwide is extremely valuable to hackers because these records not only contain financial information such as social security numbers and credit card numbers, but these records also contain some of the most private and intimate details about our medical care. As a result, the law must provide greater protections over our most valuable patient information. This article has offered both judicial and legislative solutions for how we can start to combat this problem and protect our most private patient information from the threat of a cyberattack.

249. Sweeney, supra note 68.
250. Thomson, supra note 65, at 264.