I. Introduction

During this day and age, data breach paranoia has been sweeping the nation. In 2017, Equifax, a credit report company, suffered a data breach that affected 143 million Americans. Even

1 See What is a data breach?, NORTON (Jan. 13, 2020), archived at https://perma.cc/76L2-H6CP (defining a security breach as “a security incident in which information is accessed without authorization.”); see also Chris Morris, Here’s How to Find Out if Your Email Was Once of the 773 Million Exposed in Massive Data Breach, FORTUNE (Jan. 17, 2019), archived at https://perma.cc/MR62-USXF (highlighting multiple breaches, including one of the largest data breaches in history coined “Collection #1”). Collection #1 consisted of “772,904, 991 unique emails with 21,222,975 unique passwords” from various sources. Morris, supra. This specific breach is one of many other large breaches, which includes Yahoo’s breach consisting of 3 billion user accounts, Marriott/Starwood Hotel breach of 383 million records, and LinkedIn breach of 117 million users’ information. Id. See also IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses, IBM (July 11, 2018), archived at https://perma.cc/T22W-UM8G (illuminating the 2018 Cost of Data Breach Study, sponsored by IBM Security and conducted by Ponemon Institute, that showed that the average cost of a data breach globally is 3.86 million dollars in 2018).

2 See Equifax Data Breach Settlement, FTC (Sept. 2019), archived at https://perma.cc/HN8J-WEUR (providing details about the Equifax breach including the FTC’s blog post which speaks more about the breach). See also Alex Johnson, Equifax breaks down just how bad last year’s data breach was, NBCNEWS (May 8, 2018), archived at https://perma.cc/WD6M-CS9F (revealing the that the Equifax
Facebook, the world’s most popular social media platform, recently faced a data breach of its own.3 There have been many other similar occurrences in the past few years.4 Despite the security concerns posed by such breaches, consumers continue to use online networks that may be vulnerable to hackers.5 This includes the use of mobile applications (“apps”) which carry their own inherent security risks.6 As of January 2020, there are roughly 4.41 million mobile applications breach included major security breaches of people’s passports, driver’s license, and Social Security numbers. 145.5 million Social Security numbers were compromised. Id. Hackers were able to obtain “more than 200,000 credit card number and expiration dates.” Id. Equifax attributes its security breach to a “security hole” from earlier that year that Equifax “failed to patch its systems.” Id. 3 See Mike Isaac & Sheera Frenkel, Facebook Security Breach Exposes Accounts of 50 Million Users, N.Y. TIMES (Sept. 28, 2018), archived at https://perma.cc/QK96-GUR4 (illustrating that the breach of the 50 million users of Facebook came from “attackers [who] exploited a feature in Facebook’s code to gain access to user accounts and potentially take control of them.”). There were three software flaws in the coding of Facebook that allowed the hackers to gain access to several Facebook-extension applications. Id. These flaws consisted of two bugs that “were introduced by an online tool meant to improve the privacy of users, as well as a third bug that was introduced by a tool meant to make uploading birthday videos easier. Id. 4 See Kari Paul, Everything you wanted to know about data breaches, privacy violations and hacks, MARKETWATCH (Apr. 3, 2018), archived at https://perma.cc/N35W-B57H (listing many different data breaches that happened to multiple companies, including, but not limited to, Panera Bread Co., Under Armour, Orbitz.com, and Saks Fifth Avenue). 5 See Christopher Mele, Data Breaches Keep Happening. So Why Don’t You Do Something?, N.Y. TIMES (Aug. 1, 2018), archived at https://perma.cc/28Y8-VAMP (explaining how, despite concerns about the data breaches, there is a lack of consumer action to address the issue). A research experiment discovered that many people ignored warnings that the sites they were entering were not secure. Id. After hearing about data breaches, consumers experience “breach fatigue,” and they “may adjust to this being the ‘new normal.’” Id. Further, “digital natives and younger generations may perceive their personal data . . . to never have been private” to begin with. Id. 6 See John Oats, The three most common mobile security breaches, THE TELEGRAPH (July 7, 2014), archived at https://perma.cc/A4A3-PLXN (pointing out three common mobile security breaches which consist of (1) device loss and theft; (2) malware; and (3) unsecure networks). First, device loss and theft breach may occur when someone loses their phone and a third-party then gains access to the information on that phone. Id. Second, malware technologies can compromise a device upon the downloading of an infected software. Id. This malware is then capable of “tak[ing] over a phone’s data connection, send[ing] spam emails, infect[ing] other devices on the network or even harvest[ing] passwords.” Id. Finally, unsecured Wi-Fi networks are used by hackers to trap people logging into networks at locations such as coffee shops or the airport. Id.
in the Google Play and Apple Stores combined. Despite the apparent vulnerabilities of smartphones, the public continues to use mobile apps because of their convenience and easy accessibility.

Mobile apps have made their way into the health sector as well. These health-based apps are for consumer purposes, with programs such as MyFitnessPal, Weight Watchers, and the American Red Cross’s First Aid being rated among the best health mobile apps.

---

7 See J. Clement, Number of apps available in leading app stores as of 4th quarter 2019, STATISTA (Jan. 15, 2020), archived at https://perma.cc/689M-9KS7 (providing statistical data on the current use and availability of mobile applications from smartphone application stores such as Google Play). In the span of nine months, the number of Google Play mobile apps increased by one hundred thousand. Id. See also Avery Hartmans, The most downloaded iPhone app in the world right now is one you’ve probably never heard of, BUSINESS INSIDER (May 3, 2018), archived at http://perma.cc/KXU4-2DZB (listing the top ten download application in 2018, which consisted of Tik-Tok, YouTube, WhatsApp, Facebook’s Messenger, Instagram, Facebook, WeChat, QQ, and iQiyi/Google Maps).

8 See Understanding Mobile Apps, FEDERAL TRADE COMMISSION (Feb. 2017), archived at https://perma.cc/L2DJ-N9ZZ (illuminating some reasons to use mobile applications and reasons to be cautious when using them).

9 See Eric Wicklund, Top mHealth apps as rated by doctors, MOBILE HEALTH NEWS (Jan. 20, 2015), archived at https://perma.cc/L55G-56AL [hereinafter, Top mHealth apps] (detailing the results of the HealthTap survey of its own physicians and referral physician recommendations on health and wellness apps). The apps were determined on medical validity through whether the doctor would “‘put [their] name and reputation behind it.’” Id. See generally Lee Bell, Best Health And Fitness Apps 2019, FORBES (Jan. 2, 2019), archived at https://perma.cc/9MVU-YUWB (listing ten helpful health and fitness applications that are available in 2019, which entails Beachbody on Demand, Esquared, MyFitnessPal, FIIT, Move GB, Sleep ++, Headspace, Edo, TrueBe, and RiseToday). See also Calorie Counter – MyFitnessPal, GOOGLE PLAY (Jan. 13, 2020), archived at https://perma.cc/5EB9-ZKCW (highlighting the abilities of the app, which includes being able to track the user’s food intake, exercise, and progress towards “living a happier and healthier life”).

10 See Mobile health apps, ATHENAHEALTH, (Jan. 20, 2019), archived at https://perma.cc/GXR9-NTGQ (explaining the different kinds of “eHealth” or electronic health services available, which includes mHealth for providers, mHealth for consumers, patient portals, mobile-enabled EHRs, secure text messaging, patient monitoring devices, and telemedicine). Providers use mHealth apps when making clinical decisions. Id. Mobile health apps provide consumers health information in a central source, but there are concerns about accuracy and the lack of regulation. Id. Mobile-enabled EHRs provide healthcare professionals the ability to access electronic health records (EHR) on smart phones, tablet and other mobile devices. Id. Secure text messaging is encrypted to protect the information being sent. Id. Patient monitoring devices are for use with wearable sensors to monitor health and
Many of these apps are intended to directly help with assisting people with certain health conditions. In contrast, there are also numerous mobile apps that allow patients to access their medical records directly from their healthcare providers.

These mobile health (“mHealth”) apps have the ability to mitigate the cumbersome process of obtaining one’s medical record.

for tracking patient compliance with his or her treatment. Id. Telemedicine allows providers to treat patients using “cloud-based health information technology (HIT), and other technology.” Id. See Top mHealth apps, supra note 9 (noting that the top five health apps for Android included Weight Watchers Mobile (Weight Watchers International), White Noise Lite (TM Soft), Lose It! (FitNow), First Aid (American Red Cross), and RunKeeper – GPS Track Run Walk (FitnessKeeper)). The top health application for iOS was Calorie Counter & Diet Tracker. Id.

See generally Maged N. Kamel Voulos et al., How Smartphones are Changing the Face of Mobile and Participatory Healthcare: An Overview, with Example From eCAALYX, 10 BIOMEDICAL ENGINEERING ONLINE 1 (2011) (illustrating an example of mobile application used in healthcare called the Enhanced Complete Ambient Assisted Living Experiment (“eCAALYX”), which is a monitoring system that helps elders with multiple chronic diseases). The eCAALYX serves “to act as a seamless ‘informed’ intermediary between the wearable health sensors (in a ‘smart garment’) used by the older person and the health professionals’ Internet site, by reporting to the latter (but also to the patients) alerts and measurements obtained from sensors and the geographic location.” Id. at 4.

See Device Software Functions Including Mobile Medical Applications, U.S. FED. DRUG ADMIN. (Oct. 8, 2018), archived at https://perma.cc/EF2M-ZEFE [hereinafter, Mobile Medical Applications] (establishing that mobile medical apps must “meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device.”). See also C. Lee Ventola, Mobile Devices and Apps for Health Care Professionals: Uses and Benefits, 39 PHARMACY & THERAPEUTICS 356, 356 (2014) (providing the growth of the medical use of mobile applications and their benefits to healthcare professionals). Mobile device applications can assist medical professionals with “information and time management; health record maintenance communications and consulting; reference and information gathering; patient management and monitoring; clinical decision-making; and medical education and training.” Id. See also Deborah Estrin & Ida Sim, Open mHealth Architecture: An Engine for Health Care Innovation, 330 SCI. 759, 759 (2010) (providing a way to use mHealth to benefit patients, which includes a more “open architecture”). The article goes on to explain “mHealth makes it feasible for patients to collect and share relevant data at any time, not just when they happen to visit a clinic, allowing more rapid convergence of optimal treatment.” Id.

See Chris Dimick, How to Request Your Medical Records, J. AHIMA (Mar. 1, 2017), archived at https://perma.cc/Z5EA-VZV3 (providing the process and the specific details to keep in mind for traditionally obtaining medical records from 2017). The typical steps that are taken are (1) contacting the medical care provider; (2) signing a form authorizing release of the patient’s information; (3) paying a fee
The mHealth apps serve as patient portals, allowing users to directly access their medical records without going through the traditional process.14 Regardless of the type, all mHealth apps lack a stable regulatory framework that would protect against privacy and security breaches.15 Security risks can result from a non-secure server, for the record; (4) waiting several days for the request to process; and (5) either receiving the medical records by mail or by retrieving them in person. Id. All of these steps are “to ensure a person’s sensitive health information remains private” while keeping the bar low for patients to access their information. Id. HIPAA within itself allows for medical care providers to take up to thirty days to complete a single medical record request, but most places take five to ten days to process the records. Id.

14 See Mobile health apps, supra note 10 (explaining the different kinds of “eHealth” or electronic health services available, which includes mHealth for providers and consumers, patient portals, mobile-enabled EHRs, secure text messaging, patient monitoring devices, and telemedicine). See also Eric Wicklund, Designing a Mobile Patient Portal to Boost mHealth Engagement, MHEALTH INTELLIGENCE (Nov. 1, 2017), archived at https://perma.cc/66R5-3BJ5 (stating that mobile uses of patient portals should make health information more convenient and accessible by being an “on-the-go” resource). See, e.g., Partners Patient Gateway, GOOGLE PLAY (Mar. 31, 2019), archived at https://perma.cc/URG9-6Q74 (describing how the application allow patients to review their test results, manage their appointments, message their doctor, review prescriptions, and pay their bills). Some of the mobile patient portals that hospitals have adopted include Partners Patient Gateway, Christiana Care Patient Portal, and Mission Patient Connect. Id. See also Christiana Care Patient Portal, GOOGLE PLAY (Feb. 3, 2020), archived at https://perma.cc/ME8W-WMLH (explaining the function of the app is to be “a free, secure online” service that provides patients the opportunity to “access portions of their Christiana Care health records including diagnostic test results and provider notes”). See also Mission Patient Connect, GOOGLE PLAY (Feb. 3, 2020), archived at https://perma.cc/K7HW-QXC8 (detailing a North Carolina hospital’s patient portal healthcare application as “[h]ere you can securely access your medical records 24/7, request, cancel, and reschedule upcoming appointments as well as securely communicate with your provider”).

15 See Steven R. Steinhalb et al., The Emerging Field of Mobile Health, 7 SCI. TRANSLATIONAL MED. 1, 4 (2015) (delving into the privacy and security concerns of mHealth). The United States Food and Drug Administration has, in an effort to facilitate innovation, turned to a “risk-based approach to regulatory oversight.” Id. This shift focuses solely on the use of applications “that would pose a risk to patient safety if they did not function as intended.” Id. See also Vera Lúcia Raposo, Telemedicine: The Legal Framework (Or Lack of It) in Europe, 12 GMS HEALTH TECH. ASSESS. 1, 4 (2016) (recognizing the limitations of regulation based on the “practice of telemedicine”). Obstacles that are present with regulating mHealth includes the frequent data flow and the fact that telemedicine relies on IT staff who have access to sensitive patient data. Id. at 7.
network, or application.\textsuperscript{16} Even the Health Insurance Portability and Accountability Act (“HIPAA”), is not capable of protecting mHealth users, nor will it ever be able to in its current form.\textsuperscript{17}

Though HIPAA carries weight in the medical community now, it was widely considered “better than nothing” among health reformers when its original form, the Kennedy-Kassebaum Bill, first became law.\textsuperscript{18} To make matters worse, over the past several years the United States Department of Health and Human Services (“HHS”) has been amending HIPAA by enacting rules that it hopes will solve the problem of medical-based technology breaches.\textsuperscript{19} Instead of helping the medical profession, the abundance of new rules has muddied

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{16} See Jannis Müthing et al., \textit{Server-Focused Security Assessment of Mobile Health Apps for Popular Mobile Platforms}, 21 J. MED. INTERNET RES. 1, 11–12 (2019) (explaining the possible risks with using mHealth). mHealth users have difficulty distinguishing whether the server they are accessing is the real server instead of the server of a third party. \textit{Id}. mHealth applications are at a disadvantage, because “they can (and do) hide transport security issues from their users.” \textit{Id}. It has also been observed that mHealth applications use “entirely unsecured connections or a mixture of secured and unsecured connections in communication with the same server.” \textit{Id}.
\item \textsuperscript{17} See Health Insurance Portability and Accountability Act of 1996, H.R. 3103, 104th Cong. (1996) [hereinafter HIPAA] (protecting patient’s personal medical information); see also \textit{YOUR HEALTH INFORMATION PRIVACY RIGHTS}, U.S. DEP’T OF HEALTH & HUM. SERVICES (Nov. 17, 2018), archived at https://perma.cc/P4JQ-9CT6 (setting forth the basic patient protections under HIPAA). Under HIPAA, patients who have requested a medical record must be given a copy within 30 days. \textit{Id}. If there is something wrong with the record then the medical provider must change it, and patients must be allowed to know who has seen their record. \textit{Id}. See also Barry Liss, HIPAA and Mobile Health: Where’s the App for That, N.J. LAW., Dec. 2016, at 20 (analyzing the dilemma posed by medical technology and mHealth). “Today, there is a widening gap between privacy and security on one hand and society’s voracious appetite for cutting-edge technology on the other.” \textit{Id}. As the use of mHealth products and services grows, with it comes a compliance challenge. \textit{Id}. at 24. This challenge is “not only [for] the healthcare providers who use them, but also [for] the mHealth vendors and developers who market them.” \textit{Id}.
\item \textsuperscript{19} See \textit{Combined Regulation Text of All Rules}, U.S. DEP’T OF HEALTH & HUM. SERVICES (May 12, 2017), archived at https://perma.cc/4P4L-3YS3 (listing all the amendments to HIPAA, which consists of the Privacy Rule, Security Rule, Enforcement Rule, Breach Notification Rule, and the Omnibus Rule).
\end{itemize}
\end{footnotesize}
HIPAA with confusion. Many doctors dislike HIPAA because it is “making doctors’ jobs more difficult and, in some cases, affecting current and future patient care.” Moreover, HIPAA is outdated and cannot handle the new technological advances that have arisen in the health industry. HIPAA already struggles to provide security to patient information stored in electronic health records (“EHRs”), and it is surely not equipped to protect patients using mHealth.

20 See Understanding HIPAA: A brief overview, ASS’N OF HEALTH CARE JOURNALISTS (Mar. 28, 2019), archived at https://perma.cc/M3X2-Q8CR (discussing the obstacles that HIPAA has created).

21 See Ryan Gray, How HIPAA Is Harming Patient Care, MD MAG. (Feb. 10, 2016), archived at https://perma.cc/S2G4-LCSP (showing how concerned a doctor is when trying to comply with the confusing standards of HIPAA). Dr. Gray addressed how HIPPA “has created a culture of paranoia” because the accidental sharing of patient information with the wrong doctor can lead to serious career consequences and repercussions. Id.

22 See Rob Cunningham, Old Before Its Time: HIPAA And E-Health Policy, 19 HEALTH AFFAIRS 231, 231 (2000) (identifying how the current policy-making framework is not conducive to “the realities of current [information technology]” nor is it favorable to challenges that arise from the emerging marketplace). The actions, or inactions, of Congress have further aggravated and interfered with the health care policy agenda. Id.

23 See Eric S. Pasternack, HIPAA in the Age of Electronic Health Records, 41 RUTGERS L. J. 817, 818 (2010) (critiquing HIPAA and providing that HIPAA needs to be amended to better protect patient information for electronic health records). Companies such as Google and Microsoft, who operate electronic health care systems, are not covered by HIPPA, because the “HIPPA regulations are limited to ‘covered entities.’” Id. at 827. Only the Federal Trade Commission Act and user agreements provide consumer protection. Id. See also BERNARD PETER ROBICHAU, HEALTHCARE INFORMATION PRIVACY AND SECURITY REGULATORY COMPLIANCE AND DATA SECURITY IN THE AGE OF ELECTRONIC HEALTH RECORDS 22 (Apress ed., 2014) (“Businesses knew that HIPAA didn’t have a strong enforcement mechanism, and the federal government certainly didn’t have the manpower to police the healthcare industry.”). See also Introduction to Electronic Health Records (EHRs), AAFP (Jan. 23, 2020), archived at https://perma.cc/TF8U-L96B (defining EHRs as “computer software that physicians use to track all aspects of patient care,” and explaining the history behind them). EHRs include “the practice management functions of billing, scheduling, etc.” Id. See also Jim Atherton, Development of the Electronic Health Record, 13 AM. MED. ASS’N J. ETHICS 186, 187 (2011) (noting healthcare professionals were already using digital information and communication to provide or support healthcare services by using EHRs long before the creation of mobile health apps and the enactment of HIPAA). Clinical information systems were present as early as the mid-1960s. Id. Within the span of approximately five years, Health Evaluation Logical Processing (“HELP”), Computer Stored Ambulatory
II. History

A. Before the Enactment of HIPAA

Long before HIPAA, when doctors used mostly paper in providing healthcare services, medical professionals were held by simple standards to protect patients’ confidential information. One historic standard that is still applied today is the Hippocratic Oath, which originated in ancient Greece and states as follows: “What I may see or hear in the course of the treatment or even outside of the treatment in regard to life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.” Unfortunately, the Hippocratic Oath alone was

See From the Hippocratic Oath to HIPAA: A history of patient privacy, BECKER’S HEALTH IT & CIO REPORT (Aug. 19, 2016), archived at https://perma.cc/3KC7-SV75 (overviewing the history of patient privacy through the years until the enactment of HIPAA).

See id. (describing the use of the Hippocratic oath and it protection of patient’s information long before HIPAA was enacted). See also Hippocratic Oath, U. VA HEALTH SCIENCES CTR. (2013), archived at https://perma.cc/PX3R-5W9A (quoting American Medical Association’s version of the Hippocratic Oath) (“And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in the intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets.”); Gerald L. Higgins, The History of Confidentiality in Medicine: The Physician-Patient Relationship, 35 CAN. FAM. PHYSICIAN 921, 921 (1989) (providing another translation of confidentiality portion of the Hippocratic Oath) (“And whatsoever I shall see or hear in the course of my profession in the intercourse of men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets.”). Historically, the oath creates an “an absolute duty on the physician not only to preserve the confidentiality
not enough to prevent medical professionals from releasing patients’ confidential information.26

After the birth of the United States, patient confidentiality gained another layer of protection under the United States Constitution’s Bill of Rights, which provides the right to privacy in medical records.27 In a recent case, Hancock v. County of Rensselaer,28 the Second Circuit held that “even individuals with non-stigmatizing medical conditions have a right to privacy in their medical records, even if their interest in privacy might be less.”29 Although this falls under the fundamental right to privacy, the right itself is not of medical information, but also to observe discretion about general information relating to patients to which they may become privy in social intercourse.”  "Id.  
28 See Philip Rieder et al., The end of medical confidentiality? Patients, physicians and the state in history, 42 MED. HUMAN. 149, 150 (2016) (illustrating that the Hippocratic Oath was not consistently applied by Greek physicians because it was made for the Pythagorean sect and was later only seen as a “medical reference” for the Romans). In 1810, the subjective practice of medical confidentiality from the Hippocratic Oath was replaced with the Code pénal, which criminalized medical practitioners a fine of 500 francs and up to six months in prison if they “failed to withhold confidential information about their patients.”  "Id.  There were also three major cases between the 16th and 20th centuries that highlighted the problems of confidentiality.  "Id. at 150–53. First, in the 16th century, lay authorities required physicians to disclose the names of patients who suffered from syphilis.  "Id. at 150. Second, in the 18th century, healthcare providers provided patients’ confidential information to family and friends upon request.  "Id. at 151. Finally, in the 20th century, medical professionals also revealed patients’ confidential medical information to employers and insurance companies.  "Id. at 152.  
27 See CTR. FOR DEMOCRACY & TECH., HIPAA AND HEALTH PRIVACY: MYTHS AND FACTS PART 2, 2 (2009) (debunking myths about HIPAA). The courts have determined that patients have a Constitutional right to privacy as it relates to their medical information.  "Id. The courts have further held that this right does not extend to the use and disclosure of that information by private entities.  "Id.  
28 882 F.3d 58, 61 (2d Cir. 2018) (arising out of a situation where Samaritan Hospital, a primary healthcare provider for Rensselaer County Jail’s detainees, found that a nurse of the hospital physically taped her login information inside of the nurse’s desk at the jail). The hospital later discovered that the nurse’s login information had been used by unauthorized people including the jail’s employees to access medical records of multiple non-inmate patients of the hospital.  "Id. at 62.  
29 See "Id. at 65 (holding that patient medical records are afforded privacy protections).
absolute. In Whalen v. Roe, the Supreme Court held that medical information pertaining to drug use did not fall within the constitutional “zone of privacy.” Even though there is a constitutional right to medical privacy, legislators wanted more assurance that patients’ information would be protected.

HIPAA became the successor of the Health Security Act of 1993 and 1994 after President Bill Clinton signed the Kennedy-Kassebaum Bill. The Kennedy-Kassebaum Bill had two named

30 See Hancock, 882 F.3d at 68–69 (explaining that the U.S. Supreme Court, in more than one case, has held that a “patient’s interest in medical privacy [is weighed] against the societal interest in promoting the sharing of health information for certain purposes”).


32 See id. at 600 (analyzing the state of New York’s ability to record patients’ personal information on a centralized computer from doctors’ prescription of certain drugs (i.e. Schedule II drugs) that are capable of being obtained through an unlawful market). There are three ways that public disclosure of patient information can come about. Id. First, the statute may be violated by Health Department employees who fail to maintain proper security, regardless of whether this violation was deliberate or negligent. Id. Second, if a patient or doctor is accused of violating the statute, “the stored data may be offered in evidence in a judicial proceeding.” Id. Finally, a violation may occur when a doctor, a pharmacist, or the patient “reveal[s] information on a prescription form.” Id.

33 See From the Hippocratic Oath to HIPAA: A history of patient privacy, supra note 24 (outlining the road to HIPAA).

34 See Starr, supra note 18 (questioning the passing of HIPAA’s Kennedy-Kassebaum Bill). Former health reform staffers believed that HIPAA was “[b]etter than nothing.” Id. The limitations to the bill included “not extend[ing] coverage to the uninsured, and while [prohibiting] insurance companies from refusing to renew coverage,” it also failed to place limits on what insurance companies could charge. Id. See also Robert Pear, CLINTON’S HEALTH PLAN: The Overview; CONGRESS IS GIVEN CLINTON’S PROPOSAL FOR HEALTH CARE, N.Y. TIMES (Oct. 28, 1993), archived at https://perma.cc/P9SX-PGCH (expressing the feelings of some people in regard to the passing of the Health Security Act of 1993). The 1993 Health Security Act was a 240,000-word proposal for universal health insurance as President Clinton claims would fix the issue of “United States was ‘choking on a health care system that [was] not working.’” Id. The Health Security Act of 1993 includes (1) creating regional health alliances that would collect premiums; (2) alliances that guarantee health coverage for all state residences, and if not met, the Secretary of Health and Human Services has the ability to withhold Federal money; (3) the new National Board of Health “would set a health budget for the nation and would regulate most private health insurance premiums;” (4) and most Americans would get health insurance coverage. Id. See also H.R. 3600, 103rd Cong. §1 (1st Sess. 1993-94) (establishing the Health Security Act of 1993’s goal of ensuring “individual and family security.”); see also H.R. 3600, 103rd Cong. §2 (1st Sess.
objectives: (1) Health Insurance Portability, which ensured that patients could keep health insurance between jobs; and (2) Accountability, which ensured security and confidentiality. The main focus of the Kennedy-Kassebaum Bill was on its insurance provisions, but recently the focus of HIPAA has shifted to addressing privacy and security concerns in healthcare.

1993-94) (providing that one reason the Health Security Act was created was to change the “excessive burden[s]” of the healthcare system that “confuse[d] consumers and overwhelm[ed] health care providers.”); see also H.R. 3600, 103rd Cong. § 3 (1st Sess. 1993) (establishing the purposes of the Health Security Act of 1993). The goal of the Act was to not only “guarantee comprehensive and secure health care coverage,” but also to simplify the system for both providers and consumers. Id. The Act was also geared toward controlling the cost of healthcare for those who had to pay for coverage. Id. Additionally, the Act promoted choices for individuals who were choosing health care plans and providers. Id. Further, another purpose of the Act was to “encourage all individuals to take responsibility for their health care coverage.” Id.

See Guidance, OFF. OF CORP. COMPLIANCE: THE U. CHI. MED. CTR. (Feb. 2010), archived at http://perma.cc/3RZW-FGX&A (listing the objectives of the Kennedy-Kassebaum bill that later became HIPAA). See also Dave Skidmore, UNDERSTANDING THE KASSEBAUM-KENNEDY HEALTH COVERAGE BILL, WASHINGTON POST (Aug. 19, 1996), archived at https://perma.cc/EC27-XTR9 (analyzing some of the positive and negative aspects of the Kennedy-Kassebaum Bill). At the time of the bill’s passing, it best helped those already insured, “[b]ut [did] little for the more than 40 million American who lack[ed] insurance.” Id. Further, the Act did not guarantee affordable health care. Id. However, the bill did ensure that as long as someone had health insurance for twelve months, the person would not lose their health insurance nor be charged a higher rate when changing jobs. Id. See also Franke Pallone, Health Care Reform Under the Kennedy-Kassebaum Bill: 142 Cong. Rec. H. 4170, 104th Cong. 2 (Apr. 30, 1996) (describing how, under the Kennedy-Kassebaum Act, one has the ability to “take their insurance with them” upon changing or losing a job or becoming self-employed). This “portability” provision also applies to situations regarding preexisting conditions.” Id.

See William J. Clinton, President, Signing of Kassebaum-Kennedy Bill South Lawn (Aug. 21, 1996) (transcript available in Clinton Digital Library) (celebrating the signing of the Kassebaum-Kennedy Bill and stating, “With this bill, at long last, we can seal the cracks that swallow as many as 25 million Americans who can’t get insurance or fear losing it.”); see also Peter F. Edemekong, Health Insurance Portability and Accountability Act (HIPAA), STATPEARLS (June 18, 2018), archived at https://perma.cc/QQX5-7RM9 (stating that HIPAA is also referred to as the “Kennedy-Kassebaum Act” or the “Kassebaum-Kennedy Act”).
B. HIPAA Before its “Rules”

Initially, HIPAA consisted of five main objectives: (1) protecting health insurance coverage for those who changed or lost their jobs; (2) preventing healthcare-related fraud and abuse; (3) establishing guidelines for pre-tax medical spending accounts; (4) establishing guidelines for group health plans; and (5) governing company-owned life insurance policies. Yet, only “covered entities” and their business associates are required to follow HIPAA regulations. Since its enactment, HIPAA has undergone numerous revisions to account for advancement in electronic healthcare technology. However, despite the purpose of these amendments,
HIPAA was not originally designed with the intent to protect against harms caused by electronic healthcare systems. Over the years, HIPAA has grown to include numerous Rules: (1) the Privacy Rule; (2) the Security Rule; (3) the Enforcement Rule; (4) the Omnibus Rule; and (5) the Breach Notification Rule. These Rules are specifically tailored towards improving the technological standards within the healthcare system.

C. The First Set of Technology-Based Rules: The Privacy and Security Rules

The Privacy Rule was one of the first major technology-based revisions that the HHS has made to HIPAA. At the time of the
proposal of the Privacy Rule, patients were concerned with lost privacy of their healthcare information both within and outside of the healthcare system. At the same time, the individual states had varying and inconsistent privacy standards, and the Privacy Rule was intended to make “a clear and consistent set of privacy standards [that] would improve the effectiveness and the efficiency of the health care system.” This new revision to HIPAA was designed to reduce the
concerns about the risk of disclosure or improper use of information that came from using electronic records instead of paper. At the same time, the HSS still wanted the benefits that came from using electronic information despite its risks.

As it stands now, the Privacy Rule sets specific standards for healthcare plans, healthcare associates, healthcare clearinghouses, and other healthcare providers who transmit health records electronically (“covered entities”). Yet, for healthcare providers, the use of electronic transmissions, alone, is not enough to qualify the provider as a covered entity. Instead, they must additionally “transmit health information electronically in connection with a ‘standard transaction.’” Additionally, covered entities can elect to be a “hybrid

[hereinafter 2002 STATE OF HEALTH PRIVACY] (highlighting the unevenness of the privacy protections within different states under the Privacy Rule’s predecessor, the Federal Health Privacy Rules). For example, under the Fair Information Practices Act, Mass. Gen. Law ch. 66A, § 2, Massachusetts required agencies to inform “an individual whether it maintain[ed] personal data concerning” the individual. Id. at 195. Agencies were also required to provide an individual, upon his or her request, “a list of uses made of his personal data.” Id. This list had to include “identity of all persons and organizations which have gained access to the data.” Id. In contrast, Alabama lacked any general statutes granting patients the right to see their medical records or restrict the disclosure of their records. Id. at 1.

See JOY PRITTS ET AL., supra note 45, at ii (establishing the increasing concerns that patients for the safety of their medical records).

See JUNE M. SULLIVAN, HIPAA A PRACTICAL GUIDE TO THE PRIVACY AND SECURITY OF HEALTH DATA 97 (ABA, 2004) (acknowledging the significant benefits for using information technology). These benefits include increasing the “ability to identify and treat those who are at risk for disease, conduct[ing] vital research, detect[ing] fraud and abuse, and measur[ing] and improv[ing] the quality of care delivered in the U.S.” Id.

See Summary of the HIPAA Privacy Rule, supra note 41 (outlining each of the parties covered by the Privacy Rule in detail). HHS broadly classifies “health plans” as “[i]ndividuals and group plans that provide or pay the cost of medical care are covered entities.” Id. Healthcare clearinghouses only receive “individually identifiable health information only when they are providing . . . processing services to a health plan or health care provider as a business associate.” Id. See also Administrative Simplification: Covered Entity Guidance, CMS (Apr. 16, 2019) archived at https://perma.cc/LQK2-MLHY (providing a tool for determining whether an entity falls within a “covered entity”).

See Summary of the HIPAA Privacy Rule, supra note 41 (differentiating healthcare providers from other parties covered by the Privacy Rule).

See Health Care Providers & Covered Entities, U. ARIZ. RES. GATEWAY (Apr. 16, 2019), archived at https://perma.cc/4598-QD3G (defining covered entities for the
entity,” and thus may be held to all of the HIPAA requirements.51 Nonetheless, even if a healthcare provider seeks third-party assistance during the electronic transmission of patients’ health information, not only must they still follow the standards set forth by HIPAA, they are also still responsible for meeting the requirements under the Privacy Rule.52

The Privacy Rule specifically covers “individually identifiable health information” or “protected health information” (“PHI”).53 Protected patients’ health information held by a covered entity must be disclosed both when an individual requests access to their own records, as well as when the HHS requests access in furtherance of a compliance investigation or enforcement action.54 Yet, a covered entity may, without the consent of the individual, disclose or use PHI

healthcare providers who use electronic transactions). Standard transactions are for “financial and administrative transactions relating to the provision of health care.” Id. Such transactions may include the enrollment of “an individual into a health plan, checking [their] eligibility, capturing charges, [and] producing a[n] [insurance] claim.” Id.

51 See To Whom Does the Privacy Rule Apply and Whom Will It Affect?, NAT’L INST. OF HEALTH (Apr. 16, 2019), archived at https://perma.cc/RPV5-HXGC (explaining that an entity can avoid “global application” of HIPAA’s rules if it elects to be a hybrid entity when it performs covered and non-covered functions). The healthcare provider must designate the healthcare components as stated in the Privacy Rule. Id. “If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components.” Id.

52 See Summary of the HIPAA Privacy Rule, supra note 41 (establishing that healthcare providers must follow the standards under the Privacy Rule regardless if they electronically transmit the material themselves or hire another party to do so). See also Health Care Providers & Covered Entities, supra note 50 (noting that since “a health care provider is still subject to HIPAA,” a covered entity is also subject to the Act). A covered entity is still subject to HIPAA “even if it instructs other entities . . . to submit electronic claims or other standard transactions on its behalf.” Id.

53 See Summary of the HIPAA Privacy Rule, supra note 41 (maintaining that only “identifiable” health information is protected). De-identification of health information can happen by “(1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual’s relatives, household members, and employers.” Id. The removal of such information is only adequate “if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.” Id.

54 See id. (listing the required disclosures of covered entities). Covered entities may also use an individual’s health information for treatment or payments without the individual’s authorization. Id.
if it involves a “health care operation.” If use is permitted, the health information must be limited to what is “[minimally] necessary” for the covered entity “to accomplish the intended purpose of the use, disclosure or request.” Further, the covered entity must give notice of their privacy practices to the individual whose medical information is being or can be used. The Privacy Rule also establishes that covered entities need to have reasonable safeguards in place to protect that information.

Another notable revision that the HSS made to HIPAA was the Security Standards for the Protection of Electronic Protected Health

55 See id. (listing permissible uses and disclosures of PHI). Health care operations is defined so as to include “(a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities including provider or health plan performance evaluation, credentialing, and accreditation; . . . [and] (e) business planning, development, management, and administration.” See also Summary of the HIPAA Privacy Rule, supra note 41.

56 See Summary of the HIPAA Privacy Rule, supra note 41 (explaining the requirement for the covered entities to reasonably limit the use and disclosure of health information). Further, the covered entity “must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed.” Id.

57 See Notice of Privacy Practices for Protected Health Information, U.S. DEP’T HEALTH & HUM. SERVICES (Apr. 3, 2003), archived at https://perma.cc/ZN58-CSB8 (highlighting what is necessary to ensure that covered entities provide adequate notice to patients). These privacy practices must be a clear and in plain language of how the patient’s information might be used or disclosed and along with the patient’s rights to their protected health information. Id. The content of the notice must include details about: (1) “[h]ow the covered entity may use and disclose protected health information about an individual;” (2) “[t]he individual’s rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity;” (3) “[t]he covered entity’s legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected information;” and (4) “[w]hom individuals can contact for further information about the covered entity’s privacy policies.” Id. The notice must include an effective date and must be updated when there are material changes in the privacy practices. Id. See also Summary of the HIPAA Privacy Rule, supra note 41 (outlining all the requirements that the covered entity needs to include when providing notice).

58 See Summary of the HIPAA Privacy Rule, supra note 41 (establishing that covered entities must establish and “maintain reasonable and appropriate administrative, technical, and physical safeguards” as a means of preventing both intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule). Covered entities must also limit their “incidental use and disclosure pursuant to otherwise permitted or required use of disclosure.” Id.
Information (“Security Rule”). Similar to the Privacy Rule’s PHIs, the Security Rule established standards for covered entities to protect individuals’ electronic protected health information (“e-PHI”). Both the Security Rule and the Privacy Rule had similar goals: allowing technology to make healthcare more efficient, while still protecting the privacy of individual’s healthcare information. Unlike the Privacy Rule, however, the Security Rule designed to specifically cater to electronically-stored health information.

The Security Rule had two main approaches for its safeguard standards. First, the Rule aimed to ensure that an individual’s electronic medical information was protected and secured by having an electronic signature associated with electronically transmitted

59 See Summary of the HIPAA Security Rule, U.S. DEP’T HEALTH & HUM. SERVICES (July 26, 2013), archived at https://perma.cc/C6UF-NVR8 (summarizing the key points of HIPAA’s Security Rule); see also The Security Rule, U.S. DEP’T HEALTH & HUM. SERVICES (May 12, 2017), archived at https://perma.cc/YK64-DAM2 (providing links and dates to different revisions). The proposal of the Security Rule came a year prior to the Privacy Rule but had a final revision in the year following the Privacy Rule’s last modification. Id.

60 See Summary of the HIPAA Security Rule, supra note 59 (clarifying the similarities and differences between HIPAA’s Security and Privacy Rules). Similar to the Privacy Rule, the Security Rule applies to “covered entities.” Id. However, in contrast, the Security rule caters towards the electronic health information, instead of broadly addressing the protected health information of individuals. Id.

61 See id. (explaining that, the prior to HIPAA, the health care industry lacked both a “generally accepted set of security standards” as well as “general requirements” pertaining to the protection of health information). The goal of the Security Rule was to develop flexible and scalable standards and requirements that allow a covered entity to implement policies, procedures and technologies that are tailored to its “particular size, organizational structure, and risk to consumers’ e-PHI.” Id. See also The HIPAA Privacy Rule, supra note 43 (contrasting how the Privacy Rule only requires safety measures that address privacy protections for individual, or personal, health information). The Privacy Rule also only “sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.” Id.

62 See Security and Electronic Signature Standards, 63 Fed. Reg. 43242 (proposed Aug. 12, 1998) (adopting the standards for protecting electronic health information). These new standards were adopted, because the confidentiality of electronic health information is threatened by both the risk of improper access this information as well as the risk that the information is intercepted during electronic transmission. Id.

63 See Summary of the HIPAA Security Rule, supra note 59 (“A major goal of the Security Rule is to protect the privacy of individuals’ health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.”).
health information.\textsuperscript{64} Second, the Security Rule required healthcare systems to implement three, drastically different, types of safeguards—Administrative, Physical and Technical.\textsuperscript{65} Administrative Safeguards require a current, periodic review and documentation of measures taken to ensure the protection of individual’s health information.\textsuperscript{66} In contrast, Physical Safeguards

\textsuperscript{64} See Security and Electronic Signatures Standards, 63 Fed. Reg. at 43256 (proscribing the requirements for an electronic signature to be sufficient to follow the written signature requirements that are normally proscribed by HIPAA). An electronic signature needs to (1) “[i]dentify the signatory individual;” (2) “[a]ssure the integrity of a document’s content;” and (3) “provide for nonrepudiation; that is, strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid.” Id. at 43242. See also Notice of Privacy Practices, U.S. Dep’t HEALTH & HUM. SERVICES (June 16, 2017), archived at https://perma.cc/9VGM-9UUE (disclosing that a healthcare provider must receive a signature to ensure that the individual has had notice).

\textsuperscript{65} See Summary of the HIPAA Security Rule, supra note 59 (identifying the Security Rule’s various safeguards as well as the different elements of each safeguard). Healthcare providers are encouraged to follow and conduct a specific risk analysis test. Id. This test requires healthcare providers to: (1) “[e]valuate the likelihood and impact of potential risks to e PHI;” (2) “[i]mplement appropriate security measures to address the risks identified in the risk analysis;” (3) “[d]ocument the chosen security measures and, where required, the rationale for adopting those measures;” and (4) “[m]aintain continuous, reasonable and appropriate security protections.” Id.

\textsuperscript{66} See Security and Electronic Signature Standards, 63 Fed. Reg. at 43269–72 (establishing the requirements of a “Security Management Process,” “Information Access Control,” “Security Incident Procedures,” “Contingency Plan,” and “Chain of Trust Partner Agreement” for the Administrative Safeguards). An original proposal for this safeguard, “Security Configuration Management,” required the implementation of certain practices and procedures, including, but not limited to, “documentation, hardware and/or software installation and maintenance review and testing for security features, inventory procedures, security testing, and virus checking.” Id. at 43252. See also Michael P. Barry, \textit{A Guide to the Administrative Safeguards of HIPAA’s Security Rule}, 19 \textit{Utah B. J.} 43, 44–45 (2006) (detailing the requirements for the Administrative Safeguards under HIPAA’s Security Rule). Covered entities must do a risk analysis, have risk management, have a sanction policy and maintain an information system activity review under the “Security Management Process” requirement. Id. at 44. Additionally, these entities need to appoint a Security Officer who is required to implement the security procedures. Id. Further, the companies must also provide security training awareness. Id. Business Associate agreements must also be amended to have all of the implemented safeguards stated in the Security Rule, have all of the agents of the third party agree to “implement reasonable and appropriate safeguards,” have them report to the covered entity any “attempted or successful unauthorized access, use disclosure modification, or destruction of information or interference with system operations in
require “assigned physical responsibility, media controls, physical access controls, policies and guidelines on workstation use, a secure workstation location, and security awareness training.”67 Lastly, Technical Safeguards include access controls, audit controls, data authentication, and entity authentication.68

D. The Enforcement Rule, Breach Notification Rule, and Omnibus Rule

HIPAA has three notable rules that address and enforce the purpose and goals of the Act – the Enforcement Rule, The Breach Notification Rule, and, the most recent major revision, the Omnibus Rule.69 The Enforcement and Breach Notification Rules are often less cited in comparison to the other rules of HIPAA. 70 HIPAA’s

67 See Security and Electronic Signature Standards, 63 Fed. Reg. at 43270 (providing other “Access Controls” such as workstation security, and media controls which serve as additional procedures and recovery protocols).

68 See Security and Electronic Signature Standards, 63 Fed. Reg. at 43254 (detailing the regulation’s different requirements). The Authorization Control is based on “role-based access” and “user-based access” for procuring consent. Id. Yet, the Authorization Control requirement was removed due to a fear that it would create a privacy concern rather than a security concern. Id. This requirement was intended to address the issue of workforce members being authorized to access, use and disclose health information. Id. It was not intended to address the issue of patient consent. Id.

69 See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules [hereinafter The Enforcement Rule], 78 Fed. Reg. 17,5253 (Jan. 25, 2013) (to be codified in 45 C.F.R. pts. 160, 164) (differentiating the Enforcement Rule, which provides the standards for enforcing the Privacy and Security Rules, and the Omnibus Rule, which provides the standards for enforcing the HITECH Act). 45 C.F.R. 164.400–14 (requiring covered entities and their business associates to provide notifications after a breach of unsecured protected health information has occurred).

70 See U.S. DEP’T HEALTH & HUM. SERVICES., HIPAA ADMINISTRATIVE SIMPLIFICATION: REGULATION TEXT, 45 CFR PARTS 160, 162, & 164 (Unofficial version, as amended through March 26, 2013), (2013), archived at https://perma.cc/VM3G-TVV9 [hereinafter HIPAA ADMINISTRATIVE SIMPLIFICATION] (summarizing the text for all rules that have been deemed “HIPAA
Enforcement Rule provides civil monetary penalties for violations of HIPAA’s rules.71 Meanwhile, the Breach Notification Rule enforces the requirement that medical professionals provide notification if there is a breach of protected health information.72 The Omnibus Rule was created to not only enforce the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, but also to strengthen the other three rules.73

Administrative Simplification Regulations”). These regulations include the Transactions and Code Set Standards, Identifier Standards, Privacy Rule, Security Rule, Enforcement Rule, and the Breach Notification Rule. Id.

71 See The Enforcement Rule, 78 Fed. Reg. at 5567 (providing the history and purpose of the Enforcement Rule).

72 See Breach Notification Rule, U.S. DEP’T HEALTH & HUM. SERVICES (July 26, 2013), archived at https://perma.cc/QWT9-PJDM (summarizing the requirements of notification of the Breach Notification Rule for “unsecured protected health information”). Unsecured protected health information is defined as “protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in guidance.” Id. If more than 500 residents of a state or jurisdiction are affected, then notice must be given to predominant media outlets in the area affected. Id. The Secretary must also be notified of “breaches of unsecured protected health information.” Id.

III. Facts

A. The Technology of HIPAA

The Rules of HIPAA were established in response to a push for the Act, as well as the Administrative Simplification Act, to promote efficiency in the healthcare industry. The primary goal of HIPAA was to encourage medical professionals to start using electronic means of healthcare on the premise that such methods would result in better care. More specifically, HIPAA targeted the increased use of EHRs. Yet, at the time of HIPAA’s enactment, information technology was still in its early stages of development and growth.

See Bowers, supra note 40 (noting that both the Privacy Rule and the Security Rule complement the transaction rules because their purpose is to make “the public feel more secure with electronic transmission of data”).

See Electronic Health Records, CTR. MEDICARE & MEDICAID SERVICES (Mar. 26, 2012), archived at https://perma.cc/RDH8-YEJK (identifying ways in which the health care industry benefits more from electronic healthcare systems than through the use of paper records). Such electronic healthcare systems (1) reduce medical errors “by improving the accuracy and clarity of medical records;” and (2) make patients’ health information readily available. Id. Another purpose is to implement “appropriate security safeguards” that protect vulnerable electronic health information. Id. Another purpose is to “promot[e] the use of electronic health information in the industry” through the protection of an individual’s healthcare information. Id. See also Health Insurance Portability & Accountability Act, N.H. DEP’T OF HEALTH & HUM. SERVICES (Apr. 14, 2019), archived at https://perma.cc/5ZZE-MDRL (outlining out the purposes of the security standards of HIPAA). One purpose is to implement “appropriate security safeguards” that protect vulnerable electronic health information. Id. Another purpose is to “promot[e] the use of electronic health information in the industry” through the protection of an individual’s healthcare information. Id. See also Total unit shipments of personal computers (PCs) worldwide from 2006 to 2019 (in million units), STATISTA (Jan. 21, 2019), archived at https://perma.cc/7FRG-2HQ4 [hereinafter Total unit shipments] (discussing how software development had been an important consideration during the creation of EHRs). Specifically, sufficient “[c]oding and information technology support” is necessary “to maintain the quality of the data, the running of the system, and its successful integration into the wider hospital context.” Id. See also Jo Hicks & C.J. Best, Designing Clinical Information Systems, 305 BRIT. MED. J. 776, 776 (1992) (discussing how the information technology support is capable of tackling more complex problems through either software or low use peripheral equipment).

See INTEL CORP., 1996 ANNUAL REPORT 4 (1996) [hereinafter INTEL ANNUAL REPORT] (outlining the highlights of 1996). In 1996, Intel saw connected CD-ROMs which allowed multiple player using internet to compete for games like Monopoly Interactive and the Intel Video Phone which creates video communications using telephone lines as “a revolution in progress.” Id. See also Total unit shipments, supra note 76 (showing that in 2019, 261.24 million PCs were shipped around the world).
More recently, there has been greater support by the federal government for EHRs to become the standard, as evidenced by President Bush’s plan for most Americans to have electronic health records by 2014.78 Despite this deadline, many medical professionals were, and still are, reluctant to adopt EHRs and move past paper records.79 One major concern they have about transitioning from paper records to exclusively EHRs is rooted in security issues surrounding the use of technology.80 There are several security techniques available to combat some of the risk while simultaneously complying

78 See Transforming Health Care: The President’s Health Information Technology Plan, THE WHITE HOUSE: PRESIDENT GEORGE W. BUSH (Jan. 23, 2020), archived at https://perma.cc/RKJ8-PTAV (establishing President Bush’s plan to ensure that most Americans had an electronic health record within ten years of his April 26, 2004 announcement). See also Donald W. Simborg, Promoting Electronic Health Record Adoption, Is It the Correct Focus?, 15 J. AM. MED. INFORMATICS ASS’N 127, 127 (2008) (analyzing how unsuccessful the movement had been in its efforts to get doctors on board with the use of EHRs).

79 See Simborg, supra note 78 (expressing the concern that the quality and costs of EHRs will suffer from the promotion of their adoption, as well as from the financial incentives in place to adopt them). There are numerous, enticing reasons for the physicians to switch over to EHRs. Id. For example, EHRs can lead to “[i]mproved revenue from higher Evaluation and Management (E&M) codes” and “[t]ime saving devices for physician documentation.” Id. However, increasing the use of E&M codes also leads to increases costs. Id. at 128. Despite the benefits, EHR vendors have noticed that the use of EHRs initially slows physicians down. Id. The decline in productivity, and income, appears to outweigh “[t]he fact that [EHRs] might improve [the] quality” of an individual physician’s work. Id. Further, the negative aspects of EHRs also include the possibility for fraud. Id.

80 See Clemens Scott Kruse et al., Security Techniques for the Electronic Health Records, 41 J. MED. SYST. 127, 127 (2017) (addressing security concerns and precautions taken to provide more secure EHRs). Both HIPAA and the HITECH Act provide security measures for ensuring the security and confidentiality of patients’ information. Id. at 128. HIPAA provides administrative, physical, and technical safeguards that ensure the safety of protected health information (“PHI”). Id. Security techniques under HIPAA includes the location of computers and the firewall software to protect health information. Id. Meanwhile, the HITECH Act requires medical professionals to report data breaches and for the Centers for Medicare and Medicaid Services (CMS) to implement EHRs by 2015. Id. See also Laurinda B. Harman et al., Electronic Health Records: Privacy, Confidentiality, and Security, 14 AM. MED. ASS’N J. ETHICS 712, 712 (2012) (describing the limitations of using paper health records). For example, the record is only available to one person at a time and must be updated manually, thus creating delays. Id. Additionally, paper medical records are still unsecure, as there is no security trigger or alert upon unauthorized access to a patient’s information. Id.
with HIPAA requirements. Such techniques include, but are not limited to, the use of administrative safeguards, physical safeguards, or technical safeguards.

In addition to these safeguards, HIPAA also provides specific rules targeted at addressing the abovementioned concerns. For example, the Privacy Rule was amended to specifically include cryptography as a requirement for protecting a patient’s healthcare information. Additionally, the Security Rule requires medical institutions conduct audit trails, while the HITECH Act requires these institutions to check for breaches originating from either internal or external sources. Further, HIPAA also holds employers responsible

---

81 See Kruse et al., supra note 80, at 128 (asserting that “security professionals balance their security programs with physical, technical, and administrative security controls”). The most commonly discussed of these security techniques are firewalls and cryptography. Id. Firewalls are important for protecting a medical facility’s internal network. Id. at 135. Although costly, firewalls are very successful in securing both network as a whole as well as individual patient information stored on that network. Id. Firewalls are network security device that provides a defense barrier between secured, trusted internal networks and untrusted outside networks such as the internet. See What is a Firewall?, CISCO (Nov. 21, 2018), archived at https://perma.cc/W49S-AWR7; see also Gustavus J. Simmons, Cryptology, ENCYCLOPEDIA BRITANNICA (Nov. 21, 2018), archived at https://perma.cc/BPR9-3MQT (defining cryptology as “science concerned with data communication and storage in secure and usually secret form”).

82 See Kruse et al., supra note at 80, at 133 (analyzing the different security techniques used in protecting the sensitive information contained within EHRs). Administrative safeguards include “conducting audits, assigning chief information security officer, and designing contingency plans.” Id. Physical safeguards include administrative practices as well as protection of information through hardware and software access. Id. Technical safeguards protect data and information stored within a single organization’s network. Id. Techniques for this approach include firewalls, virus checking, encryption and decryption, and authentication measures. Id. See also Harman et al., supra note 80, at 713 (furthering that a patient’s information is also protected through the access restrictions that are presented at entry, including passwords and information logins). Such restrictions for entry sometimes include “a two-tier approach to authentication,” which may involve the addition of a biometric identifier scan. Id.

83 See THE HIPAA PRIVACY RULE AND ELECTRONIC HEALTH INFORMATION EXCHANGE IN A NETWORKED ENVIRONMENT, OCR (delving into the various aspects that electronic health information is protected under HIPAA).

84 See Kruse et al., supra note 80, at 128 (detailing the requirements for HIPAA and cryptography).

85 See id. at 715 (providing how HIPAA requires that information systems activity be documented and that systems containing protected health information “the
for any employee’s misuse of a patient’s healthcare information. Yet, despite these precautions, and statutory requirements, there still is significant concern regarding the healthcare systems’ vulnerability to security breaches.

These concerns are not unprecedented, as evidenced by the 2017 breach at New York’s Bronx Lebanon Hospital Center. This breach illustrated how even when medical professionals follow the requirements of HIPAA, they can still be open to data security issues. Further, with the increased use of EHRs, there seems to be an upwards trend of health record breaches. For example, between January and

\[\text{hardware, software, and procedures to record and examine [said activity]}.\] HIPAA also requires that these audit logs be kept for a minimum of six years. 

\[\text{See Harman et al., supra note 80, at 714 (describing a case where UCLA health system employees obtained access to a patient’s confidential information). UCLA had failed to “implement security measures sufficient to reduce the risk of impermissible access to electronic protected health information by unauthorized users.” Id.}\]

\[\text{See id. at 714 (expressing the growing concerns surrounding the use of EHRs and mobile devices, due to “the rise of EHRs, medical identity theft, and a widely anticipated exchange of data between and among organizations, clinicians, federal agencies, and patients”). These concerns also arise from the sharing capabilities of these technologies and their lack of security. Id. “Mobile devices are largely designed for individual use and were not intended for centralized management by an information technology (IT) department.” Id.}\]

\[\text{See Mary Emily O’Hara, Thousands of Patient Records Leaked in New York Hospital Data Breach, NBC NEWS (May 10, 2017), archived at https://perma.cc/67TN-USPU (exposing the data breach at New York’s Bronx Lebanon Hospital Center). At least 7,000 patients’ information stored in the hospital’s EHR system was shared with an unknown third party, and it was unknown for how long their records were exposed. Id. The exposed information included “patients’ mental health and medical diagnoses, HIV status and sexual assault and domestic violence reports.” Id.}\]

\[\text{See Summary of the HIPAA Security Rule, supra note 59 (addressing that while there are numerous benefits to ERHs, the technology has limitations and vulnerabilities). HHS has also stated how “the rise in the adoption rate of these technologies [electronic health records] increases the potential security risks.” Id.}\]

\[\text{See Michela Tindera, Government Data Says Millions of Health Records Are Breach Every Year, FORBES (Sept. 25, 2018), archived at https://perma.cc/TN3A-74S6 (highlighting Massachusetts General Hospital Center for Quantitative Health’s research). The Center reviewed more than 2,000 breaches and found that between 2010 and 2017 176,4 million health records were breached. Id. During this time, there was an overall trend of increased data breaches. Id. Research has suggested data breaches may increase with the increased use of EHRs. Id. See also Linda Carroll, Health data breaches on the rise, REUTERS (Sept. 25, 2018), archived at}\]
August of 2018, there were 229 data breaches that affected 6.1 million victims.91

B. The Technology of Now

Following the rise of EHRs, telehealth communications—including mHealth apps—have grown in recent years.92 Yet, with the advancement of these apps has come serious concerns about security and privacy.93 These concerns include, but are not limited to: (1) “how
and when [a] person decide[s] whether, and with whom, to share what data and what level of granularity;” (2) “how . . . mHealth systems confidently identify individual(s) they are sensing or who is using the system;” (3) how to keep . . . health information confidential and anonymous; (4) what policies should be present; and (5) how to ensure that there is accuracy and veracity in the application’s information.94 Unlike EHRs, these answers cannot be addressed by “‘lock[ing] down’ medical devices or health records” by using firewalls and other security techniques.95 Instead, insuring the safety of protected health information must come from regulations.96

1. “Securing” Cell Phones

Although mobile phone technology has greatly improved since its inception, it is far from ensuring that the use of smart phone apps is a fully secure activity.97 The challenge of making cell phones more secure arises from the test technology companies must implement—balancing what they perceive consumers want with the limitations that keep their patients healthy through preventative care instead of only treating these patients when they become ill; (3) the quick acceptance and use of mobile health and wellness applications by patients, medical professionals, and caregivers; (4) the fact that government regulations only strive to protect medical integrity and patient privacy while there are targeted threats to health IT systems; (5) the increasing ability to hack potentially private events, such as wearable sensors in mobile devices, as the use of health technology also increases; (6) the “[h]ealthcare organization[s’] lack [of] technology and expertise to adequately secure patient data.” Id.

94 See id. (providing the answers to the abovementioned concerns).
95 See id. (reasoning that these mobile health applications cannot provide the same security measures as EHRs because mHealth applications are used “outside the clinical context and many of the wellness applications of this technology are entirely non-clinical”).
96 See EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA, U.S. DEP’T. OF HEALTH & HUM. SERVICES 1 (2016) (explaining that mHealth technologies that collect or deal in personal health records and cloud-based or mobile software tools “are outside the scope of HIPAA are referred to as “non-covered entities” or NCEs”).
97 See Justin Meyers, Watch The Incredible 70-Year Evolution Of The Cell Phone, BUSINESS INSIDER (May 6, 2011), archived at https://perma.cc/A73J-ZLTK (highlighting the vast growth of the cell phone, which has greatly reduced in size but increased in functionality).
cell phones possess. Due to its resource limitations, cell phone apps must elegantly reduce their individual footprints on a handheld device while still providing an online experience comparable to its cousin’s, the computer web browser. Despite these limitations, modern smartphones are impressive in their capabilities as they take on many heavy weight computing tasks. Nevertheless, similar to early

98 See Todd Haselton, What to look for when you’re buying a new smartphone, CNBC (Mar. 3, 2018), archived at https://perma.cc/L3VK-755T (suggesting that when choosing a mobile phone, consumers should seek larger, more pixilated, displays, longer battery life, bigger storage, and a better functioning camera); see also Suzanne Choney, What do consumers want in a cell phone?, NBC NEWS.COM (June 27, 2007), archived at https://perma.cc/78RW-RDK6 (asserting that the price, design and weight of a phone are the main priorities of a consumer who is purchasing a mobile device). See Antonio Villas-Boas, A smartphone was just announced with more RAM than a standard laptop – here’s why RAM matters on a smartphone, BUSINESS INSIDER (Dec. 11, 2018), archived at https://perma.cc/7L94-SVHE (explaining that the larger memory storage Random Access Memory (“RAM”) is a crucial to the functionality of mobile phones). Another important functionality of RAM is that it is much faster at storing information and keeping opened applications running in the background. Id. See also How Random Access Memory (RAM) affects performance, DELL (Aug. 6, 2018) [hereinafter RAM affects performance], archived at https://perma.cc/28RF-EPLG (summarizing how the mobile device needs a space to both “manipulate the data” retrieved and allow the user to interact with that data). See also Will Cell Phones Have Hard Drives, PCWORLD (Apr. 28, 2004), archived at https://perma.cc/6ATC-X23T (explaining the problems with adding a hard drive to a cell phone). Potential problems include “[c]ost, size, and power consumption. Id.

99 See Jamie Appleseed, 8 Limitations When Designing For Mobile, BAYMARD INST. (Mar. 21, 2012), archived at https://perma.cc/KXX5-RTVB (expounding on the different limitations in creating a mobile site in comparison to computer sites). These limitations include a no hover state, which is challenging for sites that have a significant amount of content or features, because the interface becomes congested with “links and buttons” that would typically only appear when hovered over. Id. Other challenges surrounding mobile versions of websites include less context, poor connectivity, and slow hardware. Id. See also Brian X. Chen, A New Phone Comes Out. Yours Slows Down. A Conspiracy? No., N.Y. TIMES (Nov. 15, 2017), archived at https://perma.cc/7Y8S-QRZY (highlighting how cell phones become bogged down when they are carrying too much data).

100 See Jeffrey Van Camp, THE 12 BEST ANDROID PHONES YOU CAN BUY IN 2019, WIRED (Mar. 5, 2019), archived at https://perma.cc/KJW9-WA45 (highlighting and describing the top smartphones of 2019). The best luxury phones had very good fingerprint sensors, wireless powerless sharing and camera capabilities. Id.
smartphones, there are still very few options for providing security protections to smartphones.\textsuperscript{101}

There are two types of software that can be utilized to make technology safer: (1) security software, and (2) protection software.\textsuperscript{102} Security software, like virus scanners, can provide security measures by acting like “security guards.”\textsuperscript{103} These virus scans are routinely done to prevent viruses and other bugs from causing harm or destruction to the system.\textsuperscript{104} In contrast, protection of the system needs

\textsuperscript{101} See Bluefire Security Technologies Supports Palm Treo 700w Smartphone, THOMAS (Apr. 26, 2006), archived at https://perma.cc/55V9-9RVL (highlighting the concern about trying to provide security to mobile phones). Bluefire Security Technologies, which is “specifically designed for mobile handheld devices,” was one of the early companies to provide security products to the Palm Treo 700w. \textit{Id. See also} Lily Hay Newman, \textit{SMARTPHONE SECURITY 101: THE STEPS THAT MATTER MOST}, WIRED (Dec. 9, 2017), archived at https://perma.cc/H6ER-ZDRZ (asserting that providing “ironclad protection” is a difficult task). Some suggested ways to protect smartphones from hackers include setting a strong pin, frequently update software, avoid third-party app stores, and paying attention to permissions for various apps. \textit{Id.}

\textsuperscript{102} See ABRAHAM SILBERSCHATZ ET AL., \textit{OPERATING SYSTEM CONCEPT ESSENTIALS} c. 13–14 (Wiley eds., 2d ed. 2014) (distinguishing protection software and security software). Security software is an added-on software that actively monitors and detects malware activity on a computer system. \textit{Id.} at 670. While protection serves for an internal problem, security includes the external environment in providing protection. \textit{Id.} at 633. A system is secure when its resources are only used and accessed for their intended purposes. \textit{Id.} at 634. In contrast, “protection” is defined as a “mechanism for controlling the access of programs, processes, or users to the resources defined by a computer system.” \textit{Id.} at 601. Protection software consists of hardware protection using the operating system such as usernames and passwords. \textit{Id.}

\textsuperscript{103} See Geoff Kuenning, \textit{How does a computer virus scan work?}, SCIENCE AMERICA (Jan. 14, 2002), archived at https://perma.cc/H54J-7YR4 (describing how virus scans work). Virus scanners search systems in an effort to detect “signatures of a known virus.” \textit{Id.} A virus scan locates the virus by looking for signature patterns that consist of the known virus. \textit{Id. See also SILBERSCHATZ ET AL., supra note 102,} at 634 (“A virus is a fragment of code embedded in a legitimate program” that are “self-replicating and are designed to ‘infect’ other programs.”). Viruses harm systems “by [both] modifying or destroying files,” as well as by causing a system to crash and a program to malfunction. \textit{Id.}

\textsuperscript{104} See SILBERSCHATZ ET AL., supra note 102, at 634 (expressing that there are two categories of security violations: (1) intentional (malicious) and (2) accidental). These kinds of security violations include (1) a breach of confidentiality, an “unauthorized reading of data (or theft of information);” (2) breach of integrity, an “unauthorized modification of data;” (3) breach of availability, an “unauthorized
to be done at four levels: physical, human, operating system, and network. Yet, despite the capabilities of both the security and protection software, HIPAA does not require, but instead merely suggests, that these software protections be utilized by healthcare systems.

2. Regulating mHealth

Since mobile apps and cell phones are still developing, there is still work to be done around improving security of these technologies, including mHealth. Currently, the FDA only regulates a small portion of health apps available to consumers, and, subsequently, there are very few regulations addressing the use of mHealth apps. In
2015, the FDA even announced that “it will not regulate informational apps that coach or prompt patients to manage their health or allow them to track their health data.” Given such restrictions, HIPAA only allows for regulation of a “covered entity” possessing a patient’s information. As a result, patients are left vulnerable to security and privacy breaches without means for recovery, as seen in the Richards v. MDLive, Inc. lawsuit.

applications). The FDA is only willing to regulate the control and adaptor applications, which “allow remote monitoring and control of medical devices” and “transform a smartphone into a medical device.” See Steinhubl et al., supra note 15, at 1 (illustrating that the healthcare industry is only now starting to incorporate mHealth technologies).

See Larson, supra note 108, at 2 (explaining how the FDA fails to regulate diagnostic applications under its 21st Century Cures Act established in 2016); see also FDA Mobile Medical Application; Guidance for Industry and Food and Drug Administration Staff; Availability, 78 Fed. Reg. 186 (proposed Sept. 25, 2013) (asserting that while “these mobile apps may meet the definition of a medical device,” the FDA intends to “exercise enforcement discretion” for these mobile apps because they pose a lower risk to the public) (emphasis added).

See Liss, supra note 17 (asserting that “the threshold inquiry regarding HIPAA compliance involves determining whether the entity that possesses the patient information is a covered entity”).

No. 0:17-CV-60760 (Fla. S.D. Ct. Apr. 18, 2017).

See id. (arising out of a claim of a client using MDLive’s mobile healthcare application based on an assertion of a breach of privacy); Class Action Complaint and Demand for Jury Trial at 7–8, Richards v. MDLive, Inc., No. 0:17-CV-60760 (Fla. S.D. Ct. Apr. 18, 2017) (asserting that Richards “relied upon MDLive’s representations that it would respect her confidentiality and take her privacy seriously by using, at minimum, industry standard security measures”). The plaintiff sought relief under 28 U.S.C. 1332 for fraud, breach of contract, or unjust enrichment and demanded to be awarded $5,000,000.00 in damages. Id. at 2. Richards had paid a $49 fee for a virtual doctor consultation, even though the application itself was free. Id. at 3. In the application, patients entered their medical history, which included health conditions, medications, allergies, behavioral health history, and family history. Id. at 2. Within the first fifteen minutes of a user opening the application, MDLive took screenshots of the user’s screen. Id. at 3. Without notifying the application user, MDLive then sent those screenshots to Test Fairy, a third-party technology company located in Israel. Id. at 6. Test Fairy claims that they use the screenshots to test for bugs and better the user’s experiences using the application. Id. See also Motion to Dismiss at 7, Richards v. MDLive, Inc., No. 0:17-CV-60760 (Fla. S.D. Ct. Apr. 18, 2017) (showing that the defendant, MDLive, argued that the consumer lacked standing to sue because they did not allege an actual injury and also failed to state a claim for relief). See also Bethany Parker, VOLUNTARY DISMISSAL BY PLAINTIFF ENDS LAWSUIT ALLEGING MDLIVE APP PRIVACY
IV. Analysis

Despite amendments to HIPAA, and advancements in technology, there remains a regulatory disconnect between the two.113 While HIPAA was a pioneer in ensuring federal compliance with the protection of patients’ confidential health information, it was never intended to cover vast and complex communications.114 Further, the amendments to HIPAA carry many holes that are not able to prevent the breach of protected information.115 As a result, it currently lacks the ability to protect information that is transmitted beyond a simple transaction between a medical professional and either their patient or another medical professional from the same facility.116

VIOLATIONS, MDLIVE (June 5, 2017), archived at http://perma.cc/JWT9-UL6S (addressing how the “lawsuit was appropriately dismissed” as MDLive’s goal is to provide “24/7/365 access to affordable virtual healthcare for consumers, employers, health plans and health systems across the U.S.”).

113 See Steinhubl et al., supra note 15 (illuminating the global uncertainty surrounding mHealth regulation). “[M]ore than 150 countries have no regulatory framework, whereas the European Union and United States are actively refining theirs.” Id.

114 See Starr, supra note 18 (hinting that despite HIPAA’s prominence as a major healthcare reform, it contains limitations).

115 See Allen B. Weisse, HIPAA: A flawed piece of legislation, 27(2) BAYLOR UNIV. MED. CTR. PROCEEDINGS 163 (2014) (establishing that absolute privacy is a “holy grail” under HIPPA, unable in practice to be achieved); see Understanding HIPAA: A brief overview, supra note 20 (pointing out that there are flaws in HIPAA). Some healthcare providers have overreacted out of fear of HIPAA’s criminal and civil penalties. Id. In contrast, other healthcare providers have simply used HIPAA as a reason to not cooperate with reporters. Id.

116 See Gray, supra note 21 (alluding that healthcare professionals have a difficult time determining what they can and cannot disclose to another provider who previously treated the same patient). While HIPAA is well-intentioned, it has “created a culture of paranoia” in the healthcare industry. Id. Medical professionals “can face serious career repercussions for accidentally sending patient information to the wrong doctor.” Id. Thus, these individuals are hesitant to “communicate with each other in cases that involve multiple patients.” Id. See also EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA, supra note 96 (addressing how despite the benefits that HIPAA provides, the scope of is “media-neutral Privacy Rule” is limited). “The wearable fitness trackers, social media sites where individuals share health information through specific social networks, and other technologies that are common today did not exist when Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191).” Id.
A. HIPAA is Not Equipped for Major Technological Changes

Although HIPAA’s primary two functions were designed to protect healthcare coverage for those who were changing jobs, or who had lost their jobs, as well as to encourage the use of electronic health systems, it has inadequately addressed the onslaught of major technological advancements.117 HIPAA’s second function arose because of the lack of participation in the push for medical professionals to use more electronic systems.118 In 1996, when HIPAA was introduced, there was only about 70 million PCs sold around the world, a number small compared to the 261.24 million PCs sold in 2019.119 The legislators sought merely to further the goal of having more doctors use electronic record systems and thus most of the technology aspect was centered around this goal.120

B. HIPAA and Electronic Health Records

Even today, HIPAA struggles to protect information stored in EHRs.121 In its current form, HIPAA and its rules serve a dual functionality; mandating certain requirements be in place while

117 See Bowers, supra note 40 (describing the primary functions of HIPAA). The core purpose of the HIPAA rules is to provide protection for individuals who have lost or who are changing their jobs. Id. HIPAA was also designed to encourage the use of electronic health systems as a means of creating more efficient health coverage. Id.
118 See id. (asserting that there would be no need for HIPAA if the entire healthcare industry had “collaborated years ago to standardize data”).
119 See INTEL ANNUAL REPORT, supra note 77 (promoting the PC sales highlights of 1996).
120 See Bowers, supra note 40 (noting that the purpose of HIPPA was to improve health coverage for patients and the healthcare industry).
121 See EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA, supra note 96, at 1 (stating that there are mHealth technologies that contain personal health records of clients that are not protected by HIPAA). Non-covered entities (“NCEs”) includes those that “are not determined to be health plans, health care clearinghouses, or health care providers conducting certain electronic transactions, and they are not acting on behalf of or providing a service to a HIPAA covered entity.” Id. at 4. These NCEs are not protected under HIPAA. Id. See Spitzer, supra note 91(not ing the frequency of security breaches while detailing one breach within a six-month window that affected 6.1 million people). See also O’Hara, supra note 88 (noting that increased EHR adoption rates increased possible security risks).
simultaneously carrying out post-damage steps. Yet, this approach does not effectively protect patients’ information. As evidenced by the New York Bronx Lebanon Hospital Center data breach, medical providers can still be susceptible to breaches and at risk of harming their patients’ security, despite following all HIPAA mandates. Additionally, the large number of breaches in the United States alone is alarming given that HIPAA’s Security and Privacy Rules were specifically implemented to prevent these kinds of harms.

HIPAA’s inability to prevent these breaches before they happen is a result, in part, of the fact that the Act remains a massive piece of legislation that many doctors struggle to fully understand.

122 See Kruse et al., supra note 80, at 131 (suggesting some ways to comply with HIPAA’s security requirements). See also The Enforcement Rule, 78 Fed. Reg. at 5566 (defining the functionality of the Enforcement Rule to provide penalties for breaching HIPAA).

123 See Breach Portal, supra note 91 (providing the public assess of the many ongoing violations of healthcare breaches). See Kruse et al., supra note 80, at 131 (opining that HIPAA’s three tier model does not encompass all versions of breaches) Many aspects of security for technology can fit within HIPAA’s three-tier model of physical, technical and administrative, however, there is no technique to thwart spurious breaches. Id. See also Liss, supra note 17 (noting the widening gap between privacy and security and the progression of technology).

124 See O’Hara, supra note 88 (stating that it was confirmed that the New York Bronx Hospital was “the target of an unauthorized hack by a third party”). Only one person was said to have unapproved access to the data. Id. Leaks similar to this are common. Id.

125 See Spitzer, supra note 91 (highlighting that in 2018 alone, there were 229 breaches over the course of only six months). Covered entities, or their business associates, are only required to send a report to the breach portal of the Civil Rights Office of the HHS when they experience a breach that is more than 500 individuals. Id. This portal is commonly coined the “wall of shame” and has been collecting information about data breaches since 2009. Id.

126 See HIPAA, supra note 17 (consisting of a wide range of rules including, but not limited to, “Prohibiting discrimination against individual participants and beneficiaries based on health status,” “Health care fraud” to “Exemption from income tax for State-sponsored workmen’s compensation reinsurance organizations”). The “[p]rohibiting [o]f discrimination against individual participants and beneficiaries based on health status” provides that a healthcare insurer cannot “establish rules for eligibility (including continued eligibility)” based on an individual’s health status or pre-existing condition. Id. at § 702. HIPAA also criminalizes “health care fraud,” which it defines, in part, as a willful or knowing execution, attempt to execute, of a scheme or artifice

(1) to defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the
Additionally, not only is the Act itself written in generic terms, but its resulting regulations are also vague. Further, these regulations are unproductive as they often contain requirements that many medical facilities have already implemented upon using new technology.

However, the implementation of vague regulations is not completely without merit as “[t]echnologies that [do not] currently exist or are impractical today” have the potential to “enhance health information security” in the future. For example, by 2003, the internet had started to become central to commerce, increasing custody or control of, any health care benefit program, in connection with the delivery of or payment for health care benefits, items, or services.

Id. at § 242. The section of the Act exempting “[s]tate-sponsored workmen’s compensation reinsurance organizations” from income tax was specifically amended to include “[a]ny membership organization if . . . such organization [was] established . . . by a State exclusively to reimburse its members for losses arising under workmen’s compensation acts.” Id. at § 342.

See Understanding HIPAA: A brief overview, supra note 20 (explaining that the regulations have generic requirements because the notice and comment period revealed that many people felt that “the security standards should not be overly prescriptive”). This view stemmed from the concern that specific requirements would become irrelevant and inapplicable due to the rapid speed at which technology is evolving, thus “deter[ing] technological progress.” Id.

See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334, 8337 (proposed Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164) (responding to the comments for more clarifications for the examples given in the Security Rule). The regulation asserts that covered entities can only determine “[their] most appropriate means of compliance” by “assessing [their] own risks” and deciding what measures are necessary to mitigate those risks. Id.

See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. at 8343 (addressing a comment calling for a more “technology-neutral approach”). The regulation’s level of detail was made with the purpose of encompassing the multitude of changes in technology. Id. at 8336. Further, the access control requirement under the Security Rule’s Technical Safeguards requires “features for emergency access procedures and provisions for context-based, role-based, and/or user-based access” but only suggests the use of encryption, which is a crucial way in securing information. Id. at 8355. This requirement was in response to a comment asserting that the individual did not want to have encryption with “[t]he use of file encryption is an acceptable method of denying access to information in that file.” Id. The comment elaborated that “[t]he use of encryption, for the purpose of access control at rest, should be based upon an entity’s risk assessment.” Id. As one of the comments in the Security Rule’s Federal Register stated, “[b]y avoiding prescription of specific technologies health care entities should use to meet the law’s requirements, you are opening the door for industry to apply innovation.” Id. at 8343.
opportunities for cyber-attacks.\textsuperscript{130} Yet, today, less than twenty years later, there are many methods available to protect the electronic-based health system, such as firewalls which can be costly but extremely effective.\textsuperscript{131} However, HIPAA’s regulatory vagueness harms the healthcare system more than it helps it, because healthcare providers are left to decide their own security protections, resulting in data breaches and leaks.\textsuperscript{132} Moreover, the relevant privacy standards are not applicable to all medical professionals, and, thus, not all patients are protected from invasions of their healthcare information.\textsuperscript{133} Therefore, despite their stated purposes, HIPAA and its subsequent regulations not only struggle to maintain the protection of EHRs, the patient information contained within them, but also fails in the face of the problems that mHealth brings forth.\textsuperscript{134}

\textsuperscript{130} See \textit{A history of Internet security}, \textsc{Washington Post} (May 30, 2015), archived at https://perma.cc/86DX-YHTX (providing an overall history of internet security). At one time, there was a security concern that with “more devices using the internet,” there would a greater opportunity for cyber-attacks. \textit{Id.} Thus, there was an additional concern that it would be more challenging to “overhaul how the system works.” \textit{Id.}

\textsuperscript{131} See Kruse et al., \textit{supra} note 80, at 131 (explaining that firewalls can be used for internal and external protection of an organization’s health records).

\textsuperscript{132} See Carroll, \textit{supra} note 90 (quoting Dr. Thomas McCoy) (“The climb in the total number of [patient healthcare] records breached is primarily attributable to very large breaches of electronic systems.”). In his research study, Dr. McCoy broke down data breaches into three categories: (1) breaches that occur at health care providers, (2) breaches that deal with health plan data, and (3) breaches of businesses associated with the health care industry. \textit{Id.} “While 70 percent of all breaches involved data stored by health care providers, the breaches involving data kept by health plans accounted for 63 percent of all stolen records.” \textit{Id.} The 510 breaches from paper and film records affected about 3.4 million patients, while the 410 breaches of network servers affected almost 140 million patients. \textit{Id.}

\textsuperscript{133} See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. at 8338 (“Only health plans, healthcare clearinghouses, and certain health care providers are required to comply with security standards.”). This regulation was in response to a comment concerning whether research organizations must follow the Security Rule even if they are affiliated with a healthcare providers. \textit{Id.}

\textsuperscript{134} See \textsc{Off. of Civ. Rts., Privacy, Security, and Electronic Health Records 2} (asserting that HIPAA’s rules were created by the Federal government to “ensure you have rights over your health information, no matter what form it is in.”). A patient’s information is protected under both HIPAA and HIPAA’s Security and Privacy Rules. \textit{Id.} See Silberschatz \textit{et al.}, \textit{supra} note 102 (describing how security can be protected within operating systems and that is often used with computers).
C. HIPAA and mHealth

Unlike computer systems, mobile applications on cell phones are still in the infancy stage of development. Subsequently, there are not that many technologies available to protect mobile applications, and there are even fewer available specifically for mHealth apps. For example, while computer systems can be protected by “firewalls,” cell phones lack access to this security option; one that has the capacity to effectively protect mHealth apps. Furthermore, not only are cell phones extremely vulnerable to security breaches, because they are connected to the internet, but cell phone users are also afforded very few legal data privacy protections. Therefore, adequate government regulation is a crucial means for securing and protecting mHealth applications, regardless of whether the apps are for consumer or professional use.

HIPAA, and other current federal regulations, offers inadequate protection for mHealth information, in part, because many mHealth apps fail to fall under any of the Act’s recognized categories and the FDA has also chosen to only regulate a small portion of health applications. For example, mHealth apps do not qualify as a

135 See Meyers, supra note 97 (expanding on the evolution of the cell phone, which grew to become the smartphone).
136 See e.g. Heathman, supra note 107 (providing seven different applications that can be used to make the use of a mobile application more secure). For example, encryption can be used to protect mobile apps through the use of other applications on the cell phone. Id.
137 See Kotz et al., supra note 93, at 2 (pointing out that healthcare systems have been traditionally secured by isolation techniques through use of tools like firewalls and network access control). “However, the trends described above make it unfeasible to simply ‘lock down’ medical devices or health-record systems, especially because patients and staff use part of the system outside of the clinical context and many of the wellness applications of this technology are entirely non-clinical.” Id.
138 See id. (stating that the risk from using devices connected to the internet is one of the security and privacy challenges).
139 Steven R. Steinhubl et al., supra note 15 (stating that there is a need for regulation based on privacy and security concerns).
140 See Summary of the HIPAA Privacy Rule, supra note 41 (explaining how HIPAA protects “individually identifiable health information” held or transmitted by a covered entity or its business associate”). This protection applies to information that is held “in any form or media,” regardless of whether it is electronic, paper or oral. Id. See also Are You a Covered Entity?, supra note 38 (qualifying who falls under what category for a covered entity). Covered entities include, but are not limited to,
covered entity, because, although they electronically transmit health information, they are not health plans, clearinghouses, or health care providers. These applications also do not qualify as a business association, because the individuals do not enter into written business agreements with a covered entity when using a mHealth app. As illustrated in Richards v. MDLive, even if an mHealth app does qualify as a covered entity, litigation regarding the misuse of patient health information is not guaranteed to be successful. However, since HIPAA removed “breaches” from its definition of “security incident,” it is unclear whether the sending of screenshots in Richards v. MDLive would be considered an “authorized” or “unauthorized” access.

If HIPAA is to continue its path of being the primary provider for security regulations for mHealth, the constant security breaches will persist, and, as a result, the list of breaches on HHS’s Breach
Portal will continue to grow.” Additionally, technology is rapidly evolving, and HIPAA not only lacks the specific requirements to prevent security breaches, but also only suggests ways in which medical providers can try to protect patient’s information. However, technology is changing too fast to simply provide a generic regulatory system.

These generic regulations make medical providers vulnerable to data breaches, because the bare protections are not enough to combat creative, and relentless, attacks by hackers, and other third-party users. The effective regulation of electronic health systems, requires a regulatory system that has the capacity to evolve with technology. Specifically, laws regulating health information must not only be specific, but also be continuously updated as a means of providing medical professionals clear guidance on what security

---

145 See Breach Portal, supra note 91 (listing the health breaches in the past two years that are under investigation for breaches of at least 500 individual’s protected health information). These breaches include, but are not limited to, hacking incidents, unauthorized access, and theft. Id. Many reported hacking incidents happened through network servers. Id. A large amount of the breaches happened through electronic means and not through paper or films. Id. See also Liss, supra note 17, at 20 (associating the possible security issues with the increase in technological advances).

146 See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. at 8336 (responding to the comments calling for less “overly prescriptive” standards). The regulation addressed how the final rule was written in such a way so as to “frame the standards” as generically as possible in a way in which they “may be met through various approaches or technologies.” Id. See also Summary of the HIPAA Privacy Rule, supra note 41 (asserting that the diversity of the health care market lead to the Rule being “designed to be flexible and comprehensive”). This flexibility allows the Rule “to cover the variety of uses and disclosures” that need to be addressed. Id.

147 See Raposo, supra note 15 (explaining the possible limitations in regulating mHealth in Europe). In European countries, “most probably the EU will only be able to create some basic guideline.” Id. “To go more in details would be problematic because until the present moment the rights of the European patient’s still lack a uniform set of rules and to start the uniformization by such a specific and domain as telemedicine.” Id.

148 See Silberschatz et al., supra note 102, at 635 (“Absolute protection of the system from malicious abuse is not possible, but the cost to the perpetrator can be made sufficiently high to deter most intruders.”). These malicious parties seek to access patient information for their own benefits. Id.

149 See Mühing et al., supra note 16 (detailing the high need for security in the use of mHealth in the server and as the protected information is transferred from one server to another).
protections they need to implement. Yet, as it stands, HIPAA will never be able to keep up with the necessary changes. Given HIPAA’s complexity, and its massive size, constant amendments to the Act will only cause more confusion and would make it harder for medical professionals to keep track of all of the current and future requirements.

D. Proposal

In establishing a law capable of protecting patients’ information while using this new technology, there must be clear boundaries limiting where patients’ information can be used and how it should be protected. As a basic guideline, application developers need to establish security measures that follow the four levels of security through physical, human, operating system, and network means. It is also essential for app developers, as well as medical providers, to implement both physical and human security measures to prevent unauthorized, third-party access to patient information. For physical security measures, the physical sites of machine rooms and terminals where the information is being stored need to be secured.

---

150 See id. ("As made evident by the comparison of the results discussed in this study with results of previous studies, the security of servers is heavily dependent on the existence and propagation of vulnerabilities.").
151 See Liss, supra note 17, at 20 (pointing to the growing need for privacy and security measures that can handle the advancement of the technology).
152 See id. at 23 ("A recent survey of healthcare providers and healthcare systems conducted by Health Information and Management Systems found that 90 percent of respondents use mobile devices to engage patients, yet only 57 percent had a mobile policy."). The FDA failed to “address at least two of the top 10 risks identified by the Open Web Application Security Project” that were of FDA-approved mHealth apps. Id.
153 See Carroll, supra note 90 (suggesting that healthcare organizations might be the easiest target or at least have the stigma being so to hackers since healthcare providers have increasingly switched to digital records).
154 See Silberschatz et al., supra note 102, at 635–36 (describing the four essential security measures).
155 See id. at 633 (pointing out that security protections needs to be for the system as well as the external environment that surrounds the system).
156 See id. at 635 (explaining the need for physical security of the site where the computer systems are located).
Most importantly, for human security, only authorized persons should be able to access patient health information.  

Additionally, users should be provided notice of data sharing through more than a third-party disclosure agreement at first use of an mHealth application.  

Ideally, mHealth apps will be held to the same standards as doctors and be required provide users with disclosures containing the names of any third parties who will have access to their records. The need for these security measures and disclosures was evidenced in Richards v. MDLive, where the third-party business associates should never have had access to the user’s information.  

Although sending screenshots was a quick and efficient way of providing feedback information, it constituted a complete disregard for the security of a user’s information.  

Furthermore, mHealth apps should contain, or be supplemented by, software that provides operating system and network protections. Such software will ensure that virus scans and other antiviral protections can search for viruses and other program threats. Finally, mHealth apps should make a practice of providing the user risk assessments.  

157. See id. at 636 (pointing out that the human security element is essential and needs to be “done carefully to assure that only appropriate users have access to the system”).  

158. See Complaint, Richards, supra note 112, at 6 (stating that the patient was unaware of the use of screenshots by MDLive used to screen for bugs).  

159. See Business Associates, supra note 38 (showing that business associates, just as doctors must routinely inform their patients that a third-party, like a laboratory or insurance company, will have access to the records).  

160. See Complaint, supra note 112, at 5 (asserting that “MDLive continuously takes screenshots of patients’ screens for the first 15 minutes after they open the app”). The number of screenshots is around sixty during the first fifteen minutes and includes the patients’ personal health information. Id. at 5-6. Knowledge of the information accessed through those screenshots does not help with fixing bugs in the app. Id.  

161. See id. at 7–8 (suggesting that the patients’ information of MDLive were given to third parties like TestFairy with little security protections).  

162. See SILBERSCHATZ ET AL., supra note 102, at 665 (expressing that under the theory of defense in depth more “layers of defense” is better than less).  

163. See id. at 670 (delving into the process of disinfecting used in antivirus programs).  

164. See id. at 666 (describing risk assessment as “attempts to value the assets of the entity in question . . . and determine the odds that a security incident will affect the entity and decrease its value”).
users of possible security risks when the app is storing certain protected health information.†65

V. Conclusion

HIPAA has become a gilded, but ultimately weak and unsteady form of health law. In its current state, HIPAA is unable to protect patients as technology rapidly advances. Legislators continue to use HIPAA as a one-size-fits-all law, adding amendments to adjust to the technology advances. Despite ongoing efforts, HIPAA was best served and used when it was for protecting patients’ insurance. HIPAA does not even have the enough means to protect patients’ EHRs, which the additional rules of HIPAA were targeted specifically to protect. Right now, mHealth applications assume that users of the applications will take precautions while and before using the applications. While HIPAA does place some guidelines for protecting patients’ information, it still allows the distribution of that information through business associates and other third parties without much notice to the patients. A new law needs to be made to specially address the rapid growth and unique security risks of modern health-related technology.

†65See id. at 666 (explaining that the best way to determine whether a security policy has been correctly implemented is through risk assessment).