UCSD UNDERGRADUATE LAW REVIEW

MEHRI SADRI

HIPAA: A Demand to Modernize Health Legislation

ABSTRACT. In the 21st-century digital age, health data privacy remains a crucial concern. This paper evaluates the effectiveness of the Health Insurance Portability and Accountability Act, known as HIPAA. More specifically, it demonstrates a need for a unified federal framework in the U.S. that aligns with General Data Protection Regulation's protections to address modern-day cybersecurity threats better. This article argues that in an era of increased globalization, the United States should confront the task of reforming its healthcare data protection law to align with current cybersecurity risks.

We begin by examining landmark legislation across American states to reveal inconsistencies between state and federal protective rulings. Later, we uncover the reactive nature of HIPAA, in contrast to GDPR's proactive and citizen-centric approach. Through evaluating past lawsuits related to patient protection noncompliance, this paper depicts significant differences in the purpose, coverage, and execution of data protection laws between the United States and the European Union. It highlights GDPR's effectiveness in granting individuals greater control over their data. Furthermore, this article proposes the adoption of newfound systems for standardized risk analysis and enhanced security across healthcare providers.

As healthcare becomes more accessible to the American public, the amount of data in this system increases. This nationwide surge in data underscores the critical need to assess whether privacy laws established in the 1990s remain sufficient. Therefore, updates to healthcare legislation are essential to establishing stringent patient protections in response to the significant rise in data breach incidents within the healthcare network.

AUTHOR. Mehri Sadri is a UC San Diego student passionate about big data security. Understanding the importance of using data for community betterment, she looks forward to fostering new discussions on how information technology infrastructure – coupled with public advocacy – can be utilized to change how user information is viewed in cyberspaces.

INTRODUCTION

Every day, thousands of Americans interact with their local or regional healthcare facilities to receive care. Often, this process consists of evaluating a simple metric, such as height and weight, at the beginning of the appointment, which a professional logs into the system's healthcare domain. When viewing a patient's health account, there is often the opportunity to see their previous health history data. A general example of this is how healthcare facilitators continuously track and document a child's increase in height and weight throughout the years. If this child moves states, their information is transferred electronically to the new provider. Information storage makes it easy to track the child's height and weight over time.

The process of completing appointments requires a patient or practitioner to request and retrieve data on patient health information. This information is stored within medical document infrastructure called Protected Health Information[1], or PHI. In an online context, the data is referred to as ePHI. As the world saw a rapid increase in technological advancement, legislation enabled government-sponsored healthcare providers, known in our discussion as covered entities, to store and protect the private health information of millions.

The federal legislation meant to safeguard ePHI is the Health Insurance Portability and Accountability Act, or HIPAA. This article focuses on two components of HIPAA: the Privacy Rule and the Security Rule.

The Privacy and Security Rule aim to protect sensitive patient health information by establishing privacy and data security standards. The Privacy Rule dictates the requirements for protecting identifiable patient information,[2] while the Security Rule focuses on safeguarding electronically Protected Health Information (ePHI) by setting criteria for its transmission and storage.[3] HIPAA was first introduced in the 1990s and fully enforced in 2003,[4] resulting in the timeline not being aligned with the increase in healthcare access.[5] Due to this outdated approach, the first section

---

[1] Digital Communications Division, What Is Phi? (last reviewed Feb. 26, 2013), What is PHI? | HHS.gov.

[2] Office for Civil Rights, Summary of the HIPPA Privacy Rule (last reviewed Oct. 19, 2022), Summary of the HIPAA Privacy Rule | HHS.gov.

[3] Office for Civil Rights, Summary of the HIPPA Security Rule (last reviewed Oct. 19, 2022), Summary of the HIPAA Security Rule | HHS.gov.

[4] Office for Civil Rights, HIPAA Compliance and Enforcement (last reviewed Jun. 28, 2021), HIPAA Compliance and Enforcement | HHS.gov.

[5] Kandyce Larson et al., Trends In Healthcare Data Breach Statistics (2014 - 2024), Healthcare Data Breach Statistics (hipaajournal.com).

of this article will analyze HIPAA's two main rules, the Privacy Act & the Security Act, while evaluating how our evolving health networks lead to core issues when enforcing these acts.

The tightening of HIPAA regulations is not only challenged by researchers wanting to freely use ePHI for innovation and advancement. Still, it is also at odds with numerous conflicting state statutes working to protect ePHI. The second section of this article will analyze the dichotomy and preemptive interaction between state laws and HIPAA's federal law related to health security and protection, and how this has played into legal settlements across different states.

The notion of protecting patient health information is not unique to the United States. The General Data Protection Regulation, or GDPR, is a European Union policy synonymous with HIPAA. However, its most significant characterizing difference concerns GDPR's broader protection of all personal data, not just health information,[6] with an emphasis on data choice and autonomy. For example, PHI can be obtained without patient consent under HIPAA, while only the party holding data can authorize release under GDPR.[7] HIPAA regulations do not give patients the authority to see where or how their data is being used, while GDPR regulations do. GDPR also enables research with secondary-source data,[8] as standards within GDPR's framework allow the sharing of anonymized data. HIPAA serves as a framework that exclusively protects patient health information, while GDPR does not apply once it has been fully anonymized.[9] The third section of this article introduces GDPR as an example of legislation more equipped to handle modern technological needs. This section will also compare the foundations of GDPR and HIPAA, demonstrating how GDPR and EU Member States have successfully solved prominent issues within HIPAA.

The United States needs practical solutions to adapt health data privacy policies to strengthen patient protection amid an increasingly technological world. This article argues that there is no single solution to strengthening patient data; instead, there should be a structured federal framework emphasizing the protection of electronic health information. With a standardized framework, private digital

[6] General Data Protection Regulation [2016] O.J. (L 119) 4.5., p. 35, art. 5.
[7] Michael Nikitin, *The Main Differences between GDPR and HIPAA*, Itirra, (Feb. 6, 2023), The Main Differences Between GDPR and HIPAA | Blog | Itirra.
[8] *Id.*
[9] Dr. Michelson discusses the secondary uses of patient data, such as research, and possible compromises to data security. Kelly N. Michelson et al., *Navigating Clinical and Business Ethics While Sharing Patient Data*, JAMA (Feb. 25, 2022).

information can be uniformly secured across all healthcare providers. This will allow states to develop common law practices and technology requirements, ratifying acts with a stricter focus based on the needs of the people.

I. HEALTH PROTECTION LEGISLATION REVIEW

A. Introducing HIPAA

The Health Insurance Portability and Accountability Act, or HIPAA, seeks to protect and "cover" three different entities: health plans, healthcare cleaning houses, and healthcare providers who transfer information from one means to another in electronic form.[10] These healthcare providers include businesses and organizations that work with patient-protected information, which HIPAA calls "Covered Entities." In order to view, share, and use patient data in broader practices like research, HIPAA's framework provides several cornerstone rules, including the Privacy Rule (last revised in 2002), the Security Rule (last revised in 2003), and the Breach Notification Act (enacted in 2009).[11] This article will focus heavily on deconstructing the Privacy and Security Rules.

HIPAA attempts to balance protecting patient information while ensuring that necessary information can be shared for patient care and scientific research.[12] However, its full list of regulations has proved costly, in both time and money, for healthcare providers to execute and the Office of Civil Rights (OCR)—tasked with enforcing HIPAA regulations—to enforce.[13] Furthermore, HIPAA regulations have been tacked onto other US healthcare procedures around informed consent, complicating essential health services and research.[14]

HIPAA commits to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings

---

[10] This article discusses how medical records are sealed by HIPAA, and possible difficulties patients might encounter while retrieving this data. Peter M. Bryniczka, *The HIPAA Hurdle* (2008), Microsoft Word - THE HIPAA HURDLE (sgbfamilylaw.com).

[11] Office for Civil Rights, *supra* note 2.

[12] Stephanie E. Pearl, *HIPAA: Caught in the Cross Fire*, 64 Duke L.J. 559, (2014).

[13] Jonathan P. Tomes, *20 plus Years of HIPAA and What Have We Got?*, 22 Quinnipiac Health L. J. 39, (2018).

[14] Mark Hochhauser, Compliance vs. Communication: Readability of HIPAA Notices (Nov., 2003), Compliance vs. Communication: Readability of HIPAA Notices (Hochhauser) | Privacy Rights Clearinghouse.

accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[15]

But it does not simplify. Instead, the full list of compliance regulations is not available in a digestible manner; rather, it is lengthy, with jargon difficult to interpret. Instead, it intends to put together components such as the Security Rule and Privacy Act, as well as other federal legislation that have developed over time.[16]

As healthcare technology emigrated from the traditional pen-and-paper period, the digitization of healthcare services accelerated the growth and accessibility of the industry. However, as the government attempts to align the lightning-speed advancements of the technological sector with archaic legislation, disasters and failure become imminent. However, such efforts have been made over the last three decades. An example can be seen in President Obama's goal to create an e-health record for American citizens including promoting IT within healthcare.[17] This plan was enacted through the 2009 American Recovery & Reinvestment Act. The statute promoted an ePHI storage method that high-tech conglomerates like Microsoft have implemented to enhance the information storage and transfer process. A more recent case of a legislative initiative to benefit social advancement and not security can be seen by President Biden's attempt at a HIPAA expansion, tied with HHS releasing a statement expressing a public-private partnership with the President in 2023, in order to protect information and accessibility to reproductive healthcare.[18] The Biden administration aimed to enforce more rigorous requirements to the PHI obtainment process. This particularly affected the forensic process of prosecution, especially in abortion/reproductive privacy cases.[19] This qualifies as growth towards HIPAA in the sense that states cannot legally request abortion-related information when being used

---

[15] *Health Insurance Portability and Accountability Act of 1996* (Aug. 20, 1996), Health Insurance Portability and Accountability Act of 1996 | ASPE (hhs.gov).

[16] Implementing a HIPAA Cybersecurity Framework, (Jun. 3, 2023), Implementing a HIPAA Cybersecurity Framework (compliancy-group.com).

[17] Danny Bradbury, *Obama and E-Health Records: Can He Really?*, Guardian, (Mar. 18, 2009, Obama and e-health records: can he really? | Health | The Guardian.

[18] Assistant Sec'y for Public Affairs, *Biden-Harris Administration Announces Public-private partnership to expand access to contraceptive care* (Jun. 21, 2023), Biden-Harris Administration Announces Public-Private Partnership to Expand Access to Contraceptive Care | HHS.gov; *see* Alice M. Ollstein, *Biden Admin to Shore up HIPAA to Protect Abortion Seekers and Providers* (Apr. 12, 2023), https://www.politico.com/news/2023/04/12/biden-admin-to-shore-up-hipaa-to-protect-abortion -seekers-and-providers-00091581.

[19] Alice M. Ollstein, *Biden's HIPAA Expansion for Abortion Draws Criticism, Lawsuit Threats*, Politico (Jul. 18, 2023), https://www.politico.com/news/2023/07/18/biden-hipaa-expansion -abortion-00106694.

as a means of prosecution. However, it alludes to a mismatch when imposing a federal law (HIPAA) that goes against state law (abortions being illegal and subject to prosecution in some states).

Once more, a legal safeguard is observed for healthcare data, aiming to shield it from third-party access, yet without enhancing the cybersecurity protocols for transferring and storing ePHI. This observation suggests that the expansions of HIPAA during the Biden and Obama administrations prioritized societal welfare influenced by social movements and motives rather than solely focusing on safeguarding ePHI amid an increasingly global network. In essence, their contributions to HIPAA appear to stem from political ideologies and economic circumstances.

Lawmakers who want to secure and safeguard ePHI should determine what is already contained within the Privacy and Security Rule and where their guidelines fail by evaluating legal settlements related to HIPAA noncompliance.

B. The Privacy Rule

The Privacy Rule, enacted in 2003[20], is a continuation of HIPAA meant to prevent unauthorized parties from receiving private health information and monitoring the "movement" of health information.[21] The rule, developed by the United States Human Health Services (HHS) department and authorized by Congress, was created to fix the "imperfections" seen in rudimentary health security legislation between 1996 and 2003. Advising and enforcing the Privacy Rule is at the discretion of the OCR, resulting in informal settlements followed by noncompliance declarations.[22] The rule was codified to cover any healthcare information used or stored for treatment and diagnosis, and the Rule defines the subclause guidelines for obtaining consent for PHI disclosure.[23] For example, The Privacy Act explains that PHI disclosure can be obtained either with written consent, informal consent, or by the covered entity

[20] Kendra Gray, *The Privacy Rule: Are We Being Deceived*, 11 Depaul Health Care L. J. 89 at 1, (2008).
[21] Emily Johnson et al., *OCR Bulletin Stresses Importance of HIPAA Compliance for Online Tracking Technology*, (Jan. 30, 2023), https://www.mcdonaldhopkins.com/insights/news/ocr-bulletin-stresses-importance-of-hipaa-compliance-for-online-tracking-technology.
[22] Myra Moran et al., *Living with the HIPAA Privacy Rule*, 32 Med. & Ethics J.L. 73, (2004).
[23] Deborah F. Buckman., *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder,* 194 A.L.R. (2004), Westlaw.

exercising "their best judgment" for the individuals' interests.[24] One example of this is the protection of patient privacy when applying for jobs or internships; a recruiter cannot legally ask a doctor to provide information on an applicant's weight or blood pressure unless there is written consent from the patient. However, when legally confronted, these definitions were too broad to accommodate increasing risks of PHI malpractice within healthcare.[25] There have been countless cases of negligent healthcare professionals dealing with sensitive information incorrectly. However, these same breaches, some worth millions, are often pardoned to ease damage from large healthcare networks.[26] Therefore, liable covered entities may feel less pressured by PHI malpractice if they believe they will be 'bailed out' by the OCR.

Compared to dealing with ePHI or cyberattacks, it seems simple for covered entities to follow rules related to patient disclosure. However, there are still issues among centers with basic noncompliance. Despite being a covered entity under HIPAA's definition, St. Joseph's Medical Center could not detect a simple breach of the Privacy Act. In 2023, the medical non-profit was ordered by OCR to pay an $80,000 penalty for its own data breach mishaps.[27] This penalty was documented as resulting from the noncompliance of three individuals' PHI[28] (medical records with clinical information) to an Associated Press reporter,[29] which was not authorized to be shared per the Privacy Rule's requirements.

---

[24] Application and compliance with the Privacy Rule. Office for Civil Rights, *supra* note 2. J ack A. Rovner et al., *Managing the Privacy Challenge: Compliance with the Amended HIPAA Privacy Rule*, 15 Health L. J. 18, (2002).

[25] Institute of Medicine et al., *Effect of the HIPAA Privacy Rule on Health Research: Proceedings of a Workshop Presented to the National Cancer Policy Forum*, Washington, DC: The National Academies Press (2006), Effect of the HIPAA Privacy Rule on Health Research: Proceedings of a Workshop Presented to the National Cancer Policy Forum | The National Academies Press.

[26] Gray, *supra* note 20.

[27] The report by the OCR mentions that St. Joseph's will be monitored for the next two years. It was reported as the 11th recorded breach. Steve Alder, *St. Joseph's Medical Center Pays $80,000 HIPAA Fine for Phi Disclosure to a Reporter* (Nov. 20, 2023), St. Joseph's Medical Center Pays $80,000 HIPAA Fine for PHI Disclosure to a Reporter (hipaajournal.com).

[28] Ricardo Pabon-Deglans, *Uses, Disclosures, and HIPAA Compliance - Disclosure of Patient Information to News Outlet,* (Jan. 9, 2024), Uses, Disclosures, and HIPAA Compliance - Disclosure of Patient Information to News Outlet | Ankura - JDSupra.

[29] The individuals' data, concerning COVID-19, was displayed for educational purposes by the Associated Press. Office for Civil Rights, *St. Joseph's Medical Center Resolution Agreement and Corrective Action Plan* (last reviewed Nov. 20, 2023), St. Joseph's Medical Center Resolution Agreement and Corrective Action Plan | HHS.gov.

C. The Security Rule

The Security Rule is vital to HIPAA, establishing a national standard for handling electronic protected health information (ePHI) during creation, retrieval, and transfer. More specific than the Privacy Rule—which covers all forms of protected health information—the Security Rule exclusively focuses on electronic records. Both rules were later additions to HIPAA, enhancing the original health information framework. The Security Rule is particularly crucial as it sets key guidelines for ePHI. It enables covered entities to develop new technologies to enhance patient care. Introduced to HIPAA in 2004, the Security Rule spans nearly 200 pages of complex legal terminology.

The Security Rule is built on three foundational principles: Confidentiality, Integrity, and Availability, which guide the use of ePHI. In its final published form, the framework of the Security Rule refers to its directives as "standards" rather than "requirements." This terminology change, made in the 2003 final publication, was intended to incorporate public feedback.[30] The verbiage of "standard" was also used in the Privacy Rule, as it gives an overview of what covered entities can do. The Security Rule should have a tighter set of restrictions that do not serve as a floor but as a dynamic, "must-follow" set of specific rules. This is because the final published version of HIPAA contrasts the Security Rule to allow "...covered entities to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission."[31] The Privacy Rule sets expectations for "what uses and disclosures are authorized or required and what rights patients have with respect to their health information." This discussion of public comment in documentation reveals that healthcare workers were in favor of looser standards due to the notion of "technology neutrality," or the idea that the Security Rule's framework can apply to a broad scope of covered entity platforms.[32] However, it is important to remember that technology was more inaccessible in 2003. Technology neutrality could be defeated by establishing a common framework and regulatory alignments across HIPAA's Security Rule, allowing for concrete rules, not baseline standards.

---

[30] Professional associations, health care workers, law firms, etc. commented on risk analysis requirements. *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (Jul. 14, 2010), rafinalguidancepdf.pdf (hhs.gov).

[31] Professional associations, health care workers, law firms, etc. commented on risk analysis requirements. *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*, Health and Human Services (Jul. 14, 2010), rafinalguidancepdf.pdf (hhs.gov).

[32] *Guidance on Risk Analysis Requirements under the HIPAA Security Rule, supra* note 31.

The Security Rule's risk analysis framework was not written for the modern era. Its confusing methodology does not clearly define "risk analysis," with no proposed metrics on frequency, etc.[33] The next two subsections will feature additional examples of HIPAA noncompliance by covered entities, drawing insight into how the Security Rule's weaknesses may have contributed.

1. Banner Health: Aftermath of Noncompliance

The Security Rule spans several pages, however. Its lengthy form is not the reason for noncompliance committed by covered entities. Sometimes, risks go unnoticed, alluding to the covered entity affecting millions of Americans. Banner Health Healthcare Company's "long-term pervasive noncompliance" court case occurred after a breach report was submitted to the OCR in 2016, resulting in an analysis of Banner Health's protection history. [34]

The data breach, which leaked the personal information of over 2.8 million patients,[35] was deemed to have been preventable if HIPAA-compliant security regulations were followed. According to the Security Rule, medical records and patient system activity should regularly be monitored[36] to check for any unauthorized access to patient health information that was not completed by the covered entity. Banner Health was unable to demonstrate that their cybersecurity adequately verified the patient accessing the PHI was truly the patient in question.[37] According to a published resolution agreement between OCR and Banner Health, the case resulted in Banner

---

[33] *Guidance on Risk Analysis Requirements under the HIPAA Security Rule, supra* note 31.
[34] David Raths, *Banner Health Settles HIPAA Security Investigation by OCR* (Feb. 6, 2023), Banner Health Settles HIPAA Security Investigation by OCR | Healthcare Innovation (hcinnovationgroup.com).
[35] Jessica Davis, *Banner Health Pays $1.25m penalty over HIPAA failures from 2016 breach*, SC Media (Feb. 2, 2023), Banner Health pays $1.25M penalty over HIPAA failures from 2016 breach | SC Media (scmagazine.com).
[36] This article outlines the specific action plans that should have been taken by Banner Health to prevent the mismanagement of ePHI. Raths, *supra* note 34.
[37] Allison Kjellander et al., *OCR Cracks Down on Electronic Protected Health Information Breaches under HIPAA* (Feb. 8, 2023), OCR Cracks Down on Electronic Protected Health Information Breaches under HIPAA | Holland & Hart LLP - JDSupra.

Health being required to develop a Corrective Action Plan to prevent such a mistake from happening again,[38] alongside two years of system monitoring.[39]

2. Impact

Despite the seven-digits penalty, within the lucrative healthcare sector, Banner Health's reported sum revenue (2022) of over $8.5 billion experienced little effect.[40] The degree of impact of OCR's CAP cannot be hard to measure, especially given that Banner Health was found guilty of another Security Rule noncompliance action unrelated to the risk analysis framework only a couple of years later.[41] With this repeat offense, it can be argued that the Security Rule's enforcement and upkeep by the OCR – both before and after the 2016 breach – was inept and, thus, negatively impacted the lives of over one million citizens. Moreover, the health professionals' comments on the Security Rule's 2003 documentation about technology neutrality do not coincide with the OCR and Banner Health's lack of enforcement. Thus, the technology neutrality can be mitigated to create stringent risk analysis requirements and that ePHI breach risk check requirements must be monitored in a stricter form: as seen by Banner Health's failure to comply twice.

It is important to note that many HIPAA violations from data breaches in the medical field have gone unnoticed. With the sheer increase in data being driven through patient care and research solutions, these numbers are expected only to grow.[42]

---

[38] The Corrective Action Plan refers to steps that must be taken when ePHI is mishandled to ensure another breech does not take place. *Resolution Agreement* (Jul. 9, 2008), TELEform Scanned document (hhs.gov).

[39] Office for Civil Rights, *OCR Settles Fourteenth Investigation in HIPAA Right of Access*, (last reviewed Jan. 12, 2023), OCR Settles Fourteenth Investigation in HIPAA Right of Access | HHS.gov.

[40] The article found that since the settlement fine was minuscule, most of Banner Health's staff and oversight were left unaffected. Andrea Suozzo et al., *Banner Health*, ProPublica (Apr. 12, 2024), Banner Health - Nonprofit Explorer - ProPublica.

[41] Raths, *supra* note 34.

[42] In this article, Heather Landi conveys the issues with HIPAA and breaches that have occurred due to its structure. The article Healthcare Data Breach Statistics comes to similar conclusions. Heather Landi, *Healthcare Data Breaches Hit All-Time High in 2021, Impacting 45M People* (Feb. 1, 2022), Healthcare data breaches hit all-time high in 2021, impacting 45M people | Fierce Healthcare; *see* Larson et al., *supra* note 5.

D. Montefiore Medical Center: Negligence Under the Security Rule

Moving forward, our analysis will focus on the Security Rule, which is specifically designed to protect patient information during electronic transfer or storage. This rule applies universally across all healthcare organizations, including small healthcare plans and any entities that handle electronic Protected Health Information (ePHI) of covered entities within the United States. Given the rising number of cyberattacks on healthcare systems, the demand to strengthen the Security Rule has become more urgent and vital than ever. The emphasis on electronic protection and the escalating cybersecurity risks in the healthcare sector make this reform particularly pertinent.[43]

The medical center was heavily penalized due to a lack of risk analysis, one of the first steps required by HIPAA's Security Rule. There is no "risk analysis" standardization when dealing with maximum coverage. According to HHS, "the [Security Rule] identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve": giving healthcare entities autonomy to perform yearly checks. Such a broad definition of an important component protecting ePH causes confusion and mishandling of data. According to an exploratory analysis of data breaches among healthcare organizations between 2015 and 2020, a vast majority of security malpractice was due to human practice and touch.[44] If medical cybersecurity transcends human technical controls, such frameworks can be incorporated into HIPAA settlement Corrective Action Plans to create a standardized system with appropriate due process.

II. STATES VERSUS HIPAA CASES

It is no secret that rules are often broken, and this applies to both electronic health information and the general healthcare process (PHI). As a federal regulation, HIPAA's framework applies to each state; however, previous cases allow us to see how

[43] Assistant Secretary for Public Affairs, *HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors* (Dec. 6, 2023), HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors | HHS.gov.

[44] Liu H. Yeo et al., *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis,* 19 Persp.s Health Info. Mgmt. (Mar. 15, 2022).

HIPAA negates state-level policies related to user data protection. This will allow us to see the state's progress over the last 30 years in protecting the increasing amount of ePHI. This section will explore how State Statutes factor into HIPAA settlement cases at the state and district levels, highlighting the conflicting friction between state and federal regulations.

A. HIPAA versus State Law Acknowledgement

HIPAA is a federal act of legislation, meaning that it works in tandem with state laws to protect the privacy and security of American citizens. Nonetheless, disparities in legislation between applying HIPAA and local state regulations add to the confusion experienced by healthcare workers and providers. Given HIPAA's extensive coverage across the federal level, it can be argued that it would be most effective to have HIPAA serve as a precursor baseline policy in an addendum to state policies tailored to local needs. State legislation can also address the many outdated conditions of HIPAA at a more expeditious pace. According to The Office of the National Coordinator for Health Information Technology (ONC), HIPAA does not override state law when it is at least as effective as HIPAA.[45] State laws contradict HIPAA if, in the absence of any exceptions, it becomes infeasible for healthcare providers to comply with HIPAA and the state directive simultaneously (due to incompatibility between the two)[46] or if the state provision hinders the achievement of HIPAA's complete objectives. For example, if a state such as California requires a consent form to be filled out by a patient for specialist visits, this would be required under state health protection law, even though HIPAA does not impose this same requirement under its jurisdiction. On the other hand, if the same specialist goes to a state that does not require these consent forms, HIPAA cannot enforce it either. This results in different laws and regulations from state to state that are hard to coordinate in interstate research or data transfer.

Knowing that HIPAA's Security Rule provides a "floorline of protection," we can now see how increased stringency in health data legislation could become a focus of states' control.

B. Analyzing California State Law towards ePHI

---

[45] *See* West Virginia Department of Health & Human Resources v. E.H, U.S. 731(2015).
[46] Robert Godard, Which Matters More: HIPAA or State Law?, I.S. Partner (Aug. 11, 2022), Which Matters More: HIPAA or State Law? (ispartnersllc.com).

California has the highest recording of healthcare data breach incidents per population size.[47] When evaluating state legislation since HIPAA's arrival, we see that California was the first US state to enact privacy laws related to data breach disclosure, even before HIPAA's arrival.[48] The California Confidentiality of Medical Information Act (CMIA) was first enacted in 1981 and broadly addresses the rights and responsibilities of medical professionals toward collecting and using medical information. Starting in the 1980s, it has since undergone several technological "advancements" through the passage of various assembly bills. California Assembly Bill 1298, passed in 2007, added further stringencies to CMIA and HIPAA. Previous regulations were meant to serve as floors, not ceilings.

An example of a significant modification to health information protection is seen in AB 1298,[49] which requires data protection to extend to all businesses or entities that perform medical treatment, even if treatment is *not* the entity's primary purpose. Thus, this law extended health protection legislation to new entities, such as websites with treatment plans and information that do not store ePHI as a main function. Furthermore, the bill covers details surrounding the speed of disclosure of a breach once detected.

The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.[50]

Even seemingly small adjustments to ePHI protection in California warrant heavy attention. As the technological boom creates new platforms, user-end procedural tasks are made easier for those who work with ePHI (e.g., medical assistants). However, this presents a larger problem when keeping up with backend protection; in other words, this is the movement and transfer of ePHI across health servers that are not directly seen.

Going into the 2020s, there were initiatives toward not ratifying further federal health protection acts in California. An example of one of these laws is The American

---

[47] Rebecca Murray-Watson, *Healthcare Data Breach Statistics* (Feb. 15, 2024), Healthcare Data Breach Statistics (hipaaguide.net).

[48] Rodika Tollefson, Which State Have the Toughest Privacy Laws? (May 20, 2019), Which states have the toughest privacy laws? | Infosec (infosecinstitute.com).

[49] California Assembly Bill 1298 amended personal data protection provisions within Section 1798 of the California Civil Code. Assem. Bill no. 1298, 2006-2007 Reg. Sess., ch. 699, 2007 Cal. Stat.

[50] *Id*. at 4

Data Privacy and Protection Act (ADPPA),[51] which established robust oversight mechanisms, ensured consumers had fundamental data privacy rights and implemented effective enforcement measures.[52] but also differences in the dichotomy (level of preemptiveness) between federal and state.

In California, there is a debate over whether the federal ADPPA should override state laws such as the CMIA. Gavin Newsom, Governor of California, and Ashkan Soltani, Executive Director of the California Privacy Protection Agency, argue that the ADPPA should not supersede CMIA. They believe that Californians are already well-protected under current state laws regarding electronic personal health information (ePHI) and that states should retain the ability to enforce stricter regulations. They argue this is crucial because state lawmaking can adapt more quickly to technological changes than the slower process of federal legislative amendments. Furthermore, while the federal government does allow states to implement stricter laws, there is no provision for the opposite scenario. Governor Newsom insists that national data privacy laws should enhance, rather than diminish, the protections offered by California's existing laws.

In order to cater to Governor Newsom and Director Soltani endorsed viewpoint of having the states dictate health security to a greater degree than HIPAA, the verbiage in healthcare legislation must stay updated. For instance, terms like “reasonable integrity” remain undefined, mirroring vague definitions found in HIPAA, such as “Covered Entity” or “Business Associate,” which were points of contention in the Banner Health lawsuit. New laws must be created fast and their verbiage must be specific enough to remove potential generalizations or conflicting language within HIPAA and ePHI protection adjacent state statute terms.

By enacting federal and state legislation, we can ensure that state laws effectively address gaps in the federal framework. Clearly defining all parties involved in the exchange of electronic personal health information (ePHI) is essential. This involves refining terms like "Covered Entity" and "Business Associate" to ensure they are not merely adjacent to but fully integrated within a dynamic ePHI security and risk analysis framework. Section 3 of the bill will provide detailed explanations and further specifics.

---

[51] Press Release, Gavin Newsom et al., *Attorney General Bonta, Governor Newsom, and CPPA File Letter Opposing Federal Privacy Preemption* (Feb. 28, 2023).
[52] *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(a)(2022).

C. Vigil v. Muir Medical Group IPA, Inc.

By evaluating the recent 2022 court case *Vigil v. Muir Medical Group IPA*, Inc.[53], we see that CMIA does not fulfill its best purpose of further strengthening HIPAA legislation and health information privacy, as it contains a structure that does not adequately strengthen the security of ePHI.

The *Vigil v. Muir Medical Group* case involved a dispute over the accused negligence of over 5,000 medical records breached and exposed years before. Simply put, this case transpired due to the plaintiff, Vigil, an employee at Muir Medical Group, claiming that CMIA had been broken, leading to another employee downloading thousands of medical records.

The case was adjudicated by California's First District Court of Appeals, beginning from the plaintiff filing after their affiliated medical group failed to secure the ePHI of patients internally. This lack of security made the contents visible to an employee, who could then illegally retain the information after leaving their employment. During the hearing, the plaintiff claimed this violated CA Civ Code § 56.36 (through 2012 Leg Sess) subdivisions within CMIA. Vigil's original motion was declined because instead of CMIA, each ePHI owner would have to show that their medical information's confidentiality has been unlawfully compromised. Furthermore, the CMIA does not apply to Vigil, as HIPAA policies trump CMIA requirements.

The plaintiff appealed the trial court's decision. In appealing, Vigil included references to Muir Medical Group breaking its own imposed HIPAA policies, given there was evidence that the ex-employee downloaded and viewed a spreadsheet with ePHI.[54] Vigil contended that the trial court failed to read and apply CMIA protections to individuals who experienced the illegal filing and handling of their ePHI. Vigil believed punishment should be based on individualized complaints instead of a common assumption, which defines that patients' medical information should be kept confidential and protected from unauthorized disclosure, the current standard in CMIA.

This case, now in the Court of Appeals, was again rejected in 2022. The case summary upheld that the trial court correctly interpreted that a breach of confidentiality requires the information to be seen and that medical information was stolen or neglected. This conclusion is amended through another case with Sutter

[53] Vigil v. Muir Medical Group IPA, Inc., No. C1801331 (Cal. Ct. App. 2022).
[54] Brief for the Petitioner, Vigil v Muir Medical Group IPA, Inc., No. C1801331 (Cal. Ct. App. 2022).

Health, finding

> The trial court denied the motion, finding as to the CMIA claim that each class member would have to show that the confidential nature of his or her medical information had been breached by an unauthorized party, as required by *Sutter Health v. Superior Court* (2014) 227 Cal.App.4th 1546 (Sutter Health), and therefore that common issues would not predominate.[55]

1. Discussion

The decision from the Court of Appeals confirmed that the California trial court correctly applied the CMIA to the situation. It also determined that the plaintiff did not demonstrate a breach of confidentiality on a "class-wide" basis. This means the plaintiff could not claim a violation of privacy on behalf of others without direct evidence. The court's decision established that a breach is only considered if there is "active viewing" of the ePHI. Consequently, in cases involving large groups—over 5,000 individuals in this instance—there must be evidence that each individual's ePHI was viewed to establish negligence. Additionally, the plaintiff is required to prove each claim of a breach individually rather than collectively. Without meeting these criteria, plaintiffs cannot certify a class action in cases of data breaches.

This ruling could potentially discourage other employees, like Vigil, from reporting suspected ePHI breaches in the workplace. Furthermore, if healthcare entities lack sufficient risk analysis or the infrastructure needed to identify and monitor these risks effectively, maintaining these legal standards could jeopardize patient safety and discourage plaintiffs.

CMIA, one of the first health data confidentiality laws, contains infrastructure and requirements that inadequately protect patient health information. Although CMIA and similarly strict laws can override HIPAA, I assert that CMIA is not using this capability to its full potential. In section 4 of this article, we will explore modern legislative proposals to create harmony between federal and state laws and their necessary amendments to keep up with innovation.

D. West Virginia Dep't of Health Services v. E.H: Stringency Applied on HIPAA

[55] *Vigil,*No. C1801331 at 2.

Two cases highlight contradictions that arise when examining the intersection of state law and HIPAA regulations. While the *Vigil* case revolves around the ambiguity of state law, the *West Virginia Department of Health Services v E.H*. defines the contradictory issue that arises from HIPAA and state legislation political disputes.[56]

With the stringency of state law taking preemptiveness with enforcement, it is oftentimes obvious to tell whether an ePHI breach court trial, for example, has a state law strictly preempting HIPAA. Through the *Vigil v. Muir Medical Group IPA*, Inc. case, we have explored what happens when this preemptive nature is unclear. Now, we will analyze a case from the state of West Virginia that shows another issue with the dichotomy between HIPAA and state law: contradictory text.

The *West Virginia Department of Health* case underscores the challenges of relying solely on federal laws like HIPAA to address evolving health data privacy and security risks. Through this case, it will once again be argued that the United States needs a more dynamic regulatory approach, including stringent state laws to fill in federal legislation gaps and adapt to technological and systemic changes.

When State law and HIPAA contradict each other, a problem is created. In 2015, a *petition* for writ of certiorari – ordering a lower court to bring up a previous case – was triggered in response to an advocacy organization, known as Legal Aid, obtaining rights to PHI from Bateman and Sharpe psychiatric facilities *without* patient consent. The Supreme Court of Appeals of West Virginia affirmed the stance in which the writ of certiorari was eventually written due to what the writ of certiorari response described as simply "HIPAA" and "a state agency's preemption analysis." This established that West Virginia state law welcoming Legal Aid's patient advocacy triumphs HIPAA.

The response to this writ of certiorari defending the state's law preempting the privacy rule was filed in 2016.[57] According to this brief, there are two core reasons for the West Virginia law's dominance:

> First, HIPAA authorizes the kind of disclosure at issue here -- release of patient health information to the patient advocates. Second, even if HIPAA did not affirmatively authorize the state law permitting the disclosures, the law would not be preempted because it falls within an exception to HIPAA's express preemption clause for "more stringent" state laws.[58]

[56] W. Va. Dep't of Health & Hum. Res. v E.H., 236 W. Va. 194 (2015).
[57] Brief for the Respondent, W. Va. Dep't of Health & Hum. Res. v E.H., (U.S. Jun. 28, 2016).
[58] *Id.* at 2.

The brief claims that West Virginia's Health and Human Services's pushback to Legal Aid, as seen in the Court of Appeals case, was met by dismay, alluding to a "popularity" viewpoint rather than a legally sound conclusion.

This highlights an interpretation of HIPAA that permits a nonprofit like Legal Aid to access patient information without consent due to accommodating state laws that supersede federal regulations. In other words, there is an interpretation of HIPAA that allows a nonprofit like Legal Aid to obtain patient information without consent because state law triumphs federal legislation. In response to the respondents' emergency motion to restore advocate access, the brief cited that "...HIPAA expressly authorizes the release of the relevant patient records to patient advocates. In a lengthy opinion, the court agreed with respondents that several provisions of the HIPPA [misspelled on case's text] Privacy Rule -- concerning the use of PHI by business associates and for healthcare operations and healthcare oversight -- affirmatively and independently allow the disclosures at issue here." [Emphasis added to highlight misspelling of HIPAA as HIPPA.]

This was the only citation in the brief with such wording merged into HIPAA that would make Legal Aid's actions acceptable.

1. Discussion

Health Security laws, federally, are not appropriate for our evolving global network.

West Virginia's state law, which precedes HIPAA, emphasizes the independence of patient advocates and the ease of accessing patient health information without written consent. This directly fosters a conflict between state and federal health regulations. Thinking about fostering a practical dichotomy between state and federal health law, we see that West Virginia's state law said to preempt HIPAA and protect advocacy organizations like Legal Aid, in this case, holds with regard to the Brief of Opposition. More specifically, the West Virginia legislature upheld that patient advocates should be independent of facility management and that written consent is unnecessary to obtain patient health information. It is significant to mention that this law was enacted in 1997, only one year after HIPAA, before the Cybernet boom we see today. Additionally, the law was written to benefit psychiatric patients without considering how patients' information would be processed or stored in just a few years.

There is an assertion that HIPAA provides exceptions when there is a

preemption for “more stringent” state laws. In this case, the law relating to releasing patient data to advocacy organizations is considered stricter than HIPAA federal law. The case underscores the broader language within HIPAA's Privacy Rule allowing disclosure to business associates, potentially increasing the risk of ePHI breaches, especially when data transfers occur remotely and associate businesses do not prioritize HIPAA compliance training.

Although contracts are required between the two parties federally, the covered entity is not required to monitor or oversee how business associates use patient data. Additionally, they are not liable if business associates misuse data.

Even more concerning is that the transfer of data from entity to associate is often done remotely. This may be detrimental to ePHI safety if the associate is not complicit with HIPAA ePHI security standards, procedures, or protocol. Increasing the visibility of ePHI might lead to more frequent small medical breaches, such as data stalking and innocent misuse among associate employees, as protected health information training may not be an associate business’s priority.

E. Conclusion and Exploring Solutions

By acknowledging the differences between state and federal law when related to ePHI security, this paper proposes that these different levels of law should work in tandem to strengthen the security measures of healthcare patients’ data. However, with the increasing flexibility in viewing and transferring patient data, there will likely be more connections between covered entities and business associates for the art of research and the overall benefit of the community. These criteria allow states to use HIPAA’s general protections, while additionally creating state-wide legislation adapted to the unique circumstances of each community.

Furthermore, there should be a greater push for adapting state legislation to serve as a HIPAA ceiling, tailored to the needs of covered entities on a state-by-state basis. By establishing focus committees at the state level to address and advise lawmakers on the best methods for risk analysis in health cybersecurity, covered entities will be subject to health protection laws that rapidly advance the protection of encrypted ePHI transfers. Additionally, states can seize the opportunity to further define terms such as "covered entity" or "business associate" based on their current legal infrastructure and future needs. This will create more standardized regulations for entities to follow, preventing confusion in a court of law.

III. GDPR & INTEGRATION

A. Introduction

The preceding sections of this article have revolved around the development of federal and state data protection legislation within the United States. However, the medical data privacy issue extends beyond international borders. European data regulations present a more comprehensive and well-versed extension to our domestic solutions. It is worth noting that any international entity handling the protected health information of American healthcare agencies must comply with HIPAA standards, underscoring the significance of other regulatory frameworks affecting millions of healthcare users worldwide.

Consequently, this section will introduce the General Data Protection Regulation (GDPR),[59] which was enacted as the European Union's data privacy law in 2018. Similar to HIPAA's nationwide scope, GDPR serves as a foundational framework upon which individual European countries can build their own regulations. However, many perceive HIPAA to lag behind GDPR in terms of stringent detail and practicality concerning protection standards.[60]

Towards the conclusion of this section, we will explore potential socioeconomic, healthcare, and consumerism trends. This analysis presents the differing perspectives on citizen privacy protection between the United States and Europe.

B. GDPR's Background

The General Data Protection Regulation was incorporated by the European Union in 2016—nearly twenty years after HIPAA's upbringing.[61] GDPR replaced the previous European act meant for personal data protection, which was ratified one year earlier than HIPAA, demonstrating how HIPAA is an outdated piece of legislation.[62]

---

[59] General Data Protection Regulation [2016] O.J. (L 119) 4.5., p. 1–88.
[60] GDPR vs HIPAA – What are the differences and how to comply, GDPR vs HIPAA – What are the differences and how to comply (iubenda.com).
[61] European Data Protection Supervisor, The History of the General Data Protection Regulation, The History of the General Data Protection Regulation | European Data Protection Supervisor (europa.eu).
[62] Věra Jourová, *How will the data protection reform help fight international crime?*, E.U. Publication Office, (Jan. 2016), https://commission.europa.eu/document/download/f4e7ef46-db4f-4f4f-b151-338f094120f1_en.

Rather than extending only to health-related information, GDPR extends protection toward all forms of personal data, including giving citizens the freedom to choose what happens to their information.[63]

Although GDPR was adopted in 2016,[64] its effects did not take legal control until 2018. Since its enactment, personal health information has been protected and structured more appropriately. Health data is defined within Article 4 of GDPR to be 'profiled' if it includes the automated processing of identifying health information, and the transfer or augmentation of ePHI from one entity to another is defined as 'processing'.[65] These specific definitions are important as they resolve data-related disputes – such as hospital conglomerates or cyber hackers using ePHI to their benefit – that have been points of conflict in legal settlements involving HIPAA legislation.

Article 9 of GDPR mentions "sensitive categories" of personal data, including biometric data, that can uniquely identify an individual's health data and more. A set of subclause conditions are presented in Article 9 that must be met for the prohibition of processing to be preempted. The clauses include similar exceptions as mentioned in HIPAA, however, the GDPR version contains more expansive exceptions for health data processing that reflect 21st-century motives for private data. These include "associations or any other not-for-profit body with a political, philosophical, religious or trade union aim...or reasons of public interest in the area of public health," emphasizing GDPR's holistic focus on public outlook.[66]

C. A Clear Divergence Between GDPR and HIPAA

Similar to GDPR's focus, HIPAA provides exceptions with 'profiled' information;[67] however, the exceptions hold less emphasis on public betterment and more on group innovation and success. This shift in purpose could have been a reason why American nonprofits such as Legal Aid faced legal bearings on their 501(c)3 work, fostering confusion among the public as to why their ePHI access was deemed permissible. Compared to 'covered entities' under the HIPAA definition, GDPR-covered organizations would have to exhaust much more stringent

[63] Mariana Sousa et al., *OpenEHR Based Systems and the General Data Protection Regulation (GDPR)*, PUB Med. 91-95, (2018).
[64] European Data Protection Supervisor, *supra* note 61.
[65] [2016] O.J. (L 119) 4.5., p. 33, art. 4 (Definition).
[66] European Data Protection Supervisor, *supra*.
[67] Data Profiling is defined as the automated processing of any personal health data. [2016] O.J. (L 119) 4.5., p. 14, Recital 71.

requirements to handle EU citizen data. As the mandatory breach notification law demonstrates,[68] GDPR requires patients to be notified of any personal data breach within 72 hours. Meanwhile, HIPAA breach notifications are only required if more than 500 people are affected. HIPAA laws give an unfair advantage to the bearers of personal information (Covered Entities) rather than the people to whom the data belongs.

D. Social & Economic Implications of GDPR

The General Data Protection Regulation and the Health Insurance Portability Act provide similar "profiling" and "processing" rules for citizens' health information. However, this section of the GDPR analysis will revisit the shortcomings of HIPAA outlined in the first two sections to analyze where GDPR surpasses HIPAA in these cases and how this can be used to HIPAA's advantage.

1. Purpose

HIPAA and GDPR have different infrastructures. HIPAA surrounds the collection, storage, and processing of personal health information. Most distinguishable from the two as different is what they define as personal data. GDPR, for example, would protect personally identifiable information such as a user's phone number or email,[69] while HIPAA only protects data in a healthcare context. Although GDPR has a broader scope, it is more stringent as it strictly defines what is allowed by those who process personal data. For example, when sharing personal data, GDPR strictly prohibits sharing personal data unless an exception in Article 9 is met.[70] HIPAA does not create this strict boundary at the beginning of its framework and allows personal information to be shared without consent for "treatment" or "betterment." It can be concluded that HIPAA maintains nearly 'neutral' verbiage, granting Covered Entities and Business Associates greater flexibilities and freedoms. For example, they are not required by HIPAA to delete ePHI upon patient request, while the 'Right to be Forgotten' plays a large role in GDPR's "power to the citizens." This is why court

[68] [2016] O.J. (L 119) 4.5., art 33, at 52[hereinafter *GDPR*].
[69] *Article 4 GDPR - Definitions, supra* note 65, at 33.
[70] *Id.* at 33.

settlement cases such as *Vigil v. Muir Medical* appear to give a disadvantaged position to the plaintiff against health providers.[71]

GDPR's 'top-down' approach of establishing safeguards for all personal health information before specifically re-enunciating health data as even *more* receptive to harm, is key to safeguarding ePHI's vulnerability to cybersecurity harms and allowing healthcare entities to understand their responsibilities.

2. Coverage

As healthcare procedures became more connected to a global web, a 1996 federal regulation made sense in the context of assuring data regulated under a Covered Entity or Business Associate – anything from medical condition ePHI transferral to payment information – is appropriately safeguarded. The objective of HIPAA was to ensure that personally identifiable health information is classified to allow for increased cyber communications – transfer of ePHI. Contrarily, GDPR is applied to privacy protection for all forms of personal data and strictly identifies health data as a sensitive form of information. More specifically, GDPR is oriented towards any organization that uses the data of EU citizens rather than strictly defining protection towards a "Covered Entity" application in the American healthcare system.

This difference in general purpose between HIPAA and GDPR is reflected in the overall structure of each legislation's framework. It can be concluded that GDPR's scope and key definitions related to health information and its broader protection of different categories of personal data are stronger methods of reflecting an interconnected society that shares data internationally.

3. State versus Federal Dichotomy

GDPR applies to the 27 member states (countries) within the European Union,[72] in which each country further imposes its laws related to personal data protection. States can provide further standards to protect data processing connected with an identifiable individual. This dynamic is synonymous with HIPAA's effect on state law, in which a "floor" is set towards protecting any information related to individuals' health status, history, payment, or contact information.

---

[71] *Vigil*, No. C1801331 at 21.

[72] Ben Wolford, *Does the GDPR apply to companies outside of the EU?*, Does the GDPR apply to companies outside of the EU? - GDPR.eu.

E. Solution

Due to HIPAA's narrower scope, I conclude it is harder to follow alongside state law because its diction contains loose language, as discussed in 'Scope' on federal law. HIPAA creates unstable infrastructure for states to add more stringent legislation related to healthcare law. For example, if HIPAA were to clearly define all *exceptions* to the prohibition of unauthorized disclosure of ePHI, then states under this federal regulations could further define these exceptions by, for example, stating further specifics regarding the types of Business Associates[73] that can and cannot have ePHI access. Having state autonomy over a solid infrastructure would give local governments the autonomy to create laws that preempt solid federal infrastructure to reflect the opinions and viewpoints of its citizens. Lastly, covered entities must be made aware of HIPAA's floor versus their state's ceiling. This can be done through proper training and simple schematics conveying federal and state input.

GDPR organically enacts this well due to the European Union consisting of numerous federal branches: there are independent countries within the European Union rather than states united under one constitution. One example is the Portuguese Data Protection Law,[74] synonymous with stronger laws like California's CCPA,[75] which provides a coordinated additional layer on top of GDPR that enhances data protection and provides valuable insight into cybersecurity. Furthermore, Portugal enacted the Comissão Nacional de Proteção de Dados (CNDP) (Portuguese Data Protection Authority),[76] a regulatory agent meant to safeguard GDPR and enforce further standards. CNDP adds an extra layer to the '72-hour rule'[77] by conducting random security audits and using stringent reporting methods to prevent breaches from occurring. On top of GDPR defining what 'personal data' is, Portugal's CNDP instated 'high-risk processing' activities to monitor potential vulnerabilities.[78]

Portugal was able to implement a greater structure for personal data usage and processing through its data officer protection program, further strengthening GDPR's

[73] West Virginia Department of Health & Human Resources v E.H., *supra* note 55.
[74] Diário da República n.º 98/1991, [Série I-A de 1991-04-29].
[75] California Consumer Privacy Act of 2018, Cal. Stat. tit. 1.81.5. § 1798.100 - 1798.199.100
[76] Diário da República, 2.ª série n.64 [Regulamento no. 310/2020 of 31 March].
[77] GDPR, *supra* note 67, at 14.
[78] Data Protected-Portugal (Feb. 2024), Data Protected Portugal | Insights | Linklaters.

articles.[79] In the United States, this could be replicated by implementing information technology officers in hospital systems, who train in managing and implementing protection systems and audits at their respective sites. Such officers should have experience in a cyber environment and be versed in federal and state ePHI policies.

ASIDE

A. OpenEHR for Risk Analysis

GDPR contains a broad framework while maintaining the ethical purpose of promoting citizens' autonomy over data. From this, it can be concluded that implementing additional frameworks and specifications can be tangibly one. This is critically important as federal legislation must keep up with technological advancements and site vulnerabilities. For these reasons, I introduce the development of Open Electronic Health Records, or OpenEHR, as an efficient layer on top of GDPR and as a guiding formality for how the Security Rule (for ePHI specifically) can be revamped to support an evolving network.

OpenEHR is a platform that provides a standardized means for healthcare providers to track patients' health information. Because of its structure, OpenEHR allows entities to communicate with one another and transfer health information safely and efficiently. Personal data storage in OpenEHR contains distinct separations to protect information best. This promotes a complete separation of EHR from identifiable demographic information while still preserving a flexible connection between the two.[80] Because of this separation, amid a data breach, the healthcare entity can ensure that a patient's medical history is not connected with their identifiable demographic information. Thus, citizens' anonymity will still be protected even if the EHR layer is breached.

By developing a consistent cybersecurity framework standard among all entities that process personal health information, we can facilitate a cleaner exchange of ePHI across all Covered Entities and foster greater consistency among healthcare applications. This, in turn, can be folded into The Security Rule to improve its structure and diminish confusion. Individual states in the US can further emphasize this framework by creating acts that enforce OpenEHR.

---

[79] *Data Protection and Transparency*, Comissão Nacional de Proteção de Dados, (Mar. 4, 2024), CNPD.

[80] Mariana Sousa, *supra* note 62.

CONCLUSION

The Health Insurance Portability Accountability Act is a series of outdated regulations that do not adequately conform to the 21st-century technological demand. The increase of individuals affected by data breaches and OCR investigations[81] will continue to rise if privacy laws are not strengthened federally and among the states. Given that both the federal government and states can enact laws protecting ePHI specifically, their regulations must work together to support a secure future.

This article contends that the United States must devise a practical approach to crafting and implementing health data privacy policies that effectively safeguard patient interests. We evaluate the ineffective CAP process and court cases highlighting HIPAA weaknesses with state impositions, demonstrating a need for stricter and more standardized laws across multiple legislative bodies.

This article argues against a one-size-fits-all solution for enhancing patient data security. Instead, a comprehensive federal framework that significantly focuses on safeguarding electronic health information in a standardized state-by-state format is introduced. GDPR and EU member states have appropriate preemptive relationships, as seen through Portugal's close attention to GDPR when ratifying an additional barrier to protect consumers. Additionally, GDPR was created more recently with an approach more aligned with the needs of citizens' ever-expanding ePHI: stringency and specificity when dealing with transferring and sharing, with users' autonomy as a priority. This article urges state lawmakers to consider introducing state laws that draw further specifications on what risk analysis infrastructure, for example, "Covered Entities," "Business Associates," and other concrete HIPAA terms.

Cybersecurity is symmetric to the growing landscape of health data. With a streamlined risk analysis platform and cyber operations among various groups of related healthcare entities, we can promote further transparency to ePHI owners regarding what happens "behind the scenes." For example, drawing clear connections between state laws and HIPAA allows HIPAA to piece together purposefully and cultivate an environment where patients feel comfortable disclosing PHI to healthcare providers for their benefit. With more confidence in their information security within back-end networks, the incentive to authorize ePHI for research, innovation, and

[81] Assistant Secretary for Public Affairs, *HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack* (Mar. 14, 2024), HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack | HHS.gov.

health experiments will be bolstered.

This article acknowledges the solid infrastructure already created to protect citizens' (health) data in the United States and abroad. Although new settlement cases are being sorted by the OCR and lawsuits related to HIPAA compliance, there is a clear progression toward awareness of the importance of cybersecurity. The United States will effectively protect health data when HIPAA's Security Act is refined, the difficulties with the pipeline between states' preemptiveness and federal jurisdiction are resolved, and the overall 'Why' of HIPAA is reframed.