iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55551

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA

Wasim Fathima Shah
Wellmark- Blue Cross Blue Shield

Abstract: ***The digital revolution has irreversibly transformed the healthcare landscape, revolutionizing the way health data is managed and raising critical questions about its protection. The seamless integration of technology has propelled healthcare into a new era of interconnectedness and data-driven innovation, presenting both unprecedented opportunities and challenges. In this context, this paper conducts a comprehensive comparative study of two pivotal regulatory frameworks: the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). These regulations, enacted on different continents, serve as cornerstones in the protection of health data and offer profound insights into the evolving landscape of data privacy and security in the digital age.The surge in digital health platforms, electronic medical records, and data-sharing networks has ushered in an era where personal health information is more vulnerable and valuable than ever before. The GDPR, a landmark legislation within the European Union, empowers individuals with control over their personal data and sets stringent standards for data protection. On the other side of the Atlantic, HIPAA plays a fundamental role in regulating health data in the United States, emphasizing the confidentiality, integrity, and availability of electronic health information.This study aims to unravel the intricate tapestry of health data protection by juxtaposing the GDPR and HIPAA. By exploring their commonalities and disparities, this analysis offers insights into the multifaceted dimensions of safeguarding health data in an interconnected world. Delving into the legal principles, individual rights, organizational responsibilities, security prerequisites, procedural intricacies, and enforcement mechanisms embedded within these frameworks, this study seeks to inform stakeholders and decision-makers about the critical nuances of health data governance.Employing a comprehensive research approach that draws from primary legal sources, scholarly interpretations, case studies, and comparative analyses, this study enriches our understanding of the intricate interplay between regulation and technology. By shedding light on the regulatory strategies of the GDPR and HIPAA, stakeholders can better navigate the intricate terrain of health data protection and contribute to the development of a privacy-respecting and technologically vibrant healthcare ecosystem.***
Keywords: GDPR, HIPAA, regulatory frameworks, electronic health records.

I. INTRODUCTION

The integration of technology into our daily lives is rapidly progressing, reshaping human activities and interactions. [1]We are currently in the midst of the fourth industrial revolution, which emphasizes the need for data usage and exchange across diverse transactions. Technological advancements lead to the extensive generation, collection, transfer, and processing of personal and organizational data, playing a routine role in various human tasks. [2] The field of healthcare is also embracing this digital transformation, relying more on technology. Innovations in technology have caused significant changes in global healthcare services and systems. The digitalization of patients' health records has greatly improved responses to medical issues and emergencies worldwide. This discussion primarily focuses on health data in the context of the modern media age.

Health data refers to records containing information about an individual's medical history, including causes, diagnoses, prognoses, treatments, and payment methods for health services. [3] The traditional approach of managing health information on paper has evolved into electronic formats. The widespread adoption of electronic medical records is now an integral part of healthcare. [4] This shift has led to more flexible and convenient ways of maintaining and accessing patients' health data.

Since an individual's health is invaluable, the protection of health information becomes crucial. Throughout history, from the time of Hippocrates, patients have maintained the right to keep their medical information private. [5] The Hippocratic Oath established the earliest documented principle of medical confidentiality. [6] Physicians are obligated to maintain and secure medical information, ensuring that patient health data remains confidential and accessible only with proper authorization. Patients also hold the right to access, obtain copies of, and correct their medical records. [7]

©IJRASET: All Rights are Reserved

In the digital era, with the continuous emergence of new technologies and associated challenges, privacy and security laws are constantly evolving to address these concerns. Health data holds both significance and vulnerability. Alongside its critical nature, there is a corresponding obligation to protect health data from breaches, compromises, losses, and misuse. To achieve this, comprehensive legislation and legal decisions are enacted to safeguard health data privacy—following a global best practice.

The term 'privacy' derives from the French word 'privaute,' implying secrecy or seclusion. [8] Privacy encompasses freedom and rights as a concept. Historically, privacy had constitutional roots in the United States. [9] It was first recognized as a human right in 1890 by Samuel Warren and Louis Brandeis, who defined it as the 'right to be left alone' in their Harvard Law Review paper, "The Right to Privacy," primarily addressing the use of cameras. [10] The right to privacy is protected by the Fourth Amendment of the US Constitution and the United Nations Universal Declaration of Human Rights (UDHR) from 1948. [11]

The European General Data Protection Regulation (GDPR) of 2018 and the US Health Insurance Portability and Accountability Act (HIPAA) are examples of data privacy and protection laws in Europe and the United States, respectively. While they differ in scope, applicability, penalties, and requirements, they share a core focus. The GDPR sets standards for safeguarding personal data, including sensitive data, with a broad approach to personal data and data controllers. In contrast, HIPAA applies more narrowly to protected health information (PHI), covered entities, and business associates. This analysis delves into these laws, primarily within the context of health information in their respective jurisdictions, examining their points of convergence and divergence, along with related matters.

II. THE GDPR

The core principles anchoring the European Union (EU) encompass freedom, democracy, equality, and the rule of law. Building upon this foundation, the EU is resolutely committed to safeguarding privacy. Privacy is regarded as a fundamental right within the EU. The Charter of Fundamental Rights of the EU grants individuals the entitlement to protection of their personal data. [12] "The GDPR gives substantial weight to this principle." [13] The GDPR, an EU regulation governing data protection and privacy, is arguably the most comprehensive legal document globally in this domain. Numerous countries, including Brazil, China, Nigeria, and certain US states like California and Virginia, have drawn inspiration from the GDPR for their own data privacy laws. In a move to safeguard the processing of individuals' personal data and ensure the free movement of such data, the EU proposed this regulation on January 25, 2012. [14] Subsequently, on May 4, 2016, the EU published the final draft of the GDPR in the Official Journal of the European Union, with enforcement beginning on May 25, 2018, replacing the 1995 data protection directive. [15] The primary objective of the GDPR was to standardize data protection rules across the EU and provide enhanced protection for data subjects. It applies specifically to the 27 EU member countries and regulates the transfer of personal data beyond the EU borders. [17] Notably, the GDPR has an extraterritorial reach, applying to data controllers outside Europe if their data processing activities occur within Europe. Interestingly, the GDPR also extends to entities in the US, encompassing businesses, nonprofits, and universities that offer goods or services to EU residents or monitor their online behavior. [18] The GDPR defines individuals who own personally identifiable data as data subjects, and the collection of data that becomes meaningful and usable as data processing. A data controller, on the other hand, is an individual, group, or body that determines the purposes and methods of processing personal data. [19] The GDPR designates an individual's health information as sensitive personal data due to its vulnerability, requiring additional legal protection and explicit consent for processing. The regulation mandates that personal data must be processed lawfully, fairly, and transparently, providing six lawful bases for processing: consent, legal obligation, contractual necessity, vital interests, public interest, and legitimate interest. Importantly, the GDPR confers eight fundamental rights on data subjects, including the right to be informed, access, rectification, erasure, restriction, data portability, objection, and freedom from automated decisions. [23].

III.THE HIPAA STATUE

In contrast to the broad scope of the GDPR, HIPAA is a US federal law that specifically regulates a subset of health information known as protected health information (PHI). President Bill Clinton signed HIPAA into law on August 21, 1996, with the main aim of enhancing the portability and accountability of health insurance coverage. [24] Also referred to as the Kennedy-Kassebaum Act, named after its key sponsors Senators Ted Kennedy and Nancy Kassebaum, HIPAA was enacted to establish national safeguards for protecting sensitive patient health data. It ensures that individuals can maintain health insurance when changing jobs, prevents coverage denial due to preexisting conditions, and eliminates job lock situations. [26] The US healthcare landscape in the 19th century was marked by numerous employers offering accident insurance, which expanded with the introduction of employer-sponsored plans. However, these plans were governed by inconsistent state laws, prompting the need for federal intervention.

The Employee Retirement Income Security Act (ERISA) of 1974 addressed some issues but left gaps, primarily applying to specific health plans. Commercial for-profit health plans remained regulated by various state laws, leading to job lock situations. Congress responded by enacting HIPAA in 1996, which aimed not only to address health insurance issues but also to combat fraud, waste, and abuse, and streamline health insurance transactions. [30] Similar to the GDPR's treatment of sensitive data, HIPAA designates PHI as sensitive individual data, subject to extra safeguards to prevent misuse, discrimination, and unauthorized disclosure. It plays a critical role in safeguarding individuals' health information and promoting electronic health records and health information technology. PHI refers to identifiable personal information held or transmitted electronically or in other forms and mediums, encompassing medical records and other health-related data. PHI includes identifiers like name, birth date, social security number, and more. While HIPAA primarily applies to covered entities within the US—health plans, health clearinghouses, and healthcare providers that transmit electronic health information—it is notable that HIPAA was not primarily conceived as a privacy legislation. The "P" in HIPAA stands for "portability," emphasizing the accessibility of health insurance despite changes in employment. The US Department of Health and Human Services (HHS) developed regulations to address privacy and security of health data.

IV. THE HIPAA RULES

Within the framework of HIPAA, the Department of Health and Human Services (HHS) holds the authority to formulate regulations aimed at simplifying administrative processes in healthcare, including the electronic exchange, privacy, and security of individuals' health information. [38] Over the last two decades, HHS has issued a series of regulations to facilitate these objectives. The key rules are outlined as follows:

A. The Privacy Rule

HHS introduced the initial comprehensive privacy regulation to implement Title II, Subtitle F of HIPAA in December 2000, and it took effect on April 14, 2003, with the purpose of safeguarding the privacy of individually identifiable health information (IIHI). The Privacy Rule was deemed necessary as Congress did not pass a privacy law within the stipulated three years after enacting HIPAA. Primarily, the Privacy Rule established national standards for safeguarding protected health information (PHI). This rule aims to balance individuals' interests in maintaining the confidentiality of their health data during various private and public activities. Health information is considered protected under this rule if it meets certain criteria, including being created or received by a covered entity or employer, relating to an individual's physical or mental health, and identifying or potentially identifying the individual. [39] The central focus of the Privacy Rule is to regulate the situations involving the use and disclosure of PHI by entities subject to it. It encompasses the use, disclosure, and request for PHI, excluding specific cases such as educational records, employment records, and deceased individuals' health information held by covered entities and business associates. A business associate is an entity or person that processes PHI on behalf of a covered entity. The Privacy Rule requires a covered entity to establish a business associate agreement before disclosing PHI to such entities. This agreement outlines permissible uses and disclosures of PHI by the business associate. [41] The rule provides instances where using and disclosing PHI is necessary for healthcare services, and patient authorization isn't required. Covered entities and business associates can use and disclose PHI for treatment, payment, and healthcare operations without explicit patient consent. Additionally, the rule permits use and disclosure of PHI without prior authorization under 12 public benefit exceptions. However, for all other cases, written authorization from the patient is required, and the minimum necessary rule should be followed. [42] The Privacy Rule grants patients specific rights regarding their PHI, including the right to notice of privacy practices, access to their PHI, requesting amendment of their PHI, receiving an accounting of PHI disclosures, requesting restrictions on PHI use and disclosure, receiving confidential communications, and lodging complaints with covered entities and HHS. The Office for Civil Rights (OCR) within HHS is responsible for enforcing this rule by conducting investigations, audits, and imposing penalties.

Importantly, the Privacy Rule preempts state laws that conflict with federal standards unless the state law provides more stringent privacy protections. A state law won't be considered contrary to the federal Privacy Rule if it's needed to prevent fraud or abuse, report health costs, regulate controlled substances, monitor health plans, or address public health functions, among other specific purposes.

B. The Security Rule

From a regulatory compliance perspective, securing electronic data is pivotal to building client trust for entities and individuals. As part of the administrative simplification process, HHS published the Security Rule on February 20, 2023, with the aim of establishing national safeguards to protect the confidentiality, integrity, and availability of electronic PHI against unauthorized access, use, or disclosure.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

While the Privacy Rule applies to PHI in any medium, the Security Rule primarily concerns electronic PHI. [45] Initially applying to covered entities, the HIPAA Final Rule extended the Security Rule's requirements to business associates. [46] Entities subject to the Security Rule must implement security measures based on factors such as business size, technical infrastructure, and potential risks to electronic PHI. [47] Importantly, a security breach doesn't necessarily equate to a Security Rule breach. Compliance requires covered entities and business associates to adopt administrative, physical, and technical safeguards to protect electronic PHI. Administrative safeguards encompass policies and procedures to select, develop, implement, and maintain security measures, including security management processes to prevent, detect, contain, and correct security violations. [49] Physical safeguards relate to facility access controls, workstation use policies, workstation and device security, and media controls. Technical safeguards encompass access controls, audit controls, integrity controls, and transmission security. [52] Documentation of policies and procedures is required. The OCR is tasked with enforcing the Security Rule, similar to the Privacy Rule.

C. The Breach Notification Rule

This rule mandates covered entities and business associates to notify individuals, HHS, and sometimes the media in the event of a breach of unsecured PHI, compromising its privacy and security. [53] Unsecured PHI refers to data that unauthorized persons can access, with only encryption and destruction being approved methods to secure PHI. The rule provides exceptions to its breach definition. Covered entities must issue notice without a risk assessment in the event of a breach. If a risk assessment reveals low probability of compromise, notification isn't required. If a breach involves secured PHI, notice isn't necessary. Specific requirements for breach assessment, notification timelines, and content are outlined.

D. The Enforcement Rule

This rule outlines procedures for compliance, investigation, hearings, and penalties for Privacy and Security Rule violations. It establishes the OCR to enforce HIPAA provisions through complaint investigations, compliance reviews, and education programs. OCR collaborates with the Department of Justice for criminal breaches.

E. The Final Rule

Also known as the Omnibus Rule, this 2012 publication expanded Privacy, Security, and Breach Notification Rules to strengthen PHI privacy and security. It extended HIPAA scope to include business associates and imposed additional requirements on both covered entities and business associates, along with increased penalties.

F. HITECH Act

Enacted in 2009 as part of the American Recovery and Reinvestment Act, the HITECH Act promotes the meaningful adoption of health data technology, focusing on improving electronic health records and related technology implementation in the US. The Act reinforces existing HIPAA Rules, mandates accounting for PHI disclosures, increases penalties for violations, and allows state attorneys general to bring civil actions for violations.

V. COMMON GROUNDS BETWEEN GDPR AND HIPAA

Based on the preceding discussion, it becomes apparent that both legislations are established to safeguard sensitive personal data. Nonetheless, due to distinct focus, nuances, and requirements shaped by the diverse jurisdictions and industries they pertain to, both laws share notable similarities in terms of their scope, application, implementation, and enforcement. The prominent resemblances between these regulatory frameworks are outlined as follows:

A. Data Privacy and Protection

Both regulations are tailored to ensure the privacy and security of personal information pertaining to individuals, rather than legal entities. GDPR defines personal data in relation to any identifiable or identified natural person, whether directly or indirectly, through attributes such as name, identification number, location data, online identifiers, or factors specific to the individual's physical, psychological, genetic, mental, economic, cultural, or social identity. [55] Similarly, although HIPAA isn't a comprehensive privacy law, it safeguards Protected Health Information (PHI), encompassing individually identifiable health data. Both regulations treat health data as sensitive personal information necessitating heightened legal safeguards, given the potential for embarrassment or discrimination. Consequently, both laws recognize the necessity of obtaining an individual's consent or authorization to process, use, or disclose their sensitive information.

Both laws also require entities subject to them to implement suitable and relevant technological measures to secure personal data or PHI against improper or unauthorized use, disclosure, or access. These measures include risk or privacy impact assessments, sanction policies, monitoring, access controls, and encryption. [58]

B. Extraterritorial Application

While the world is often referred to as a global village, this extends beyond just the realms of the internet and telecommunications to encompass commerce and trade. [59] Numerous corporations and business entities engage in cross-border operations, leading to the utilization, exchange, or processing of personal data. Both GDPR and HIPAA primarily apply within specific jurisdictions—the EU and the US, respectively.

Nevertheless, both regulations can exhibit extraterritorial applicability, extending beyond their designated regions. GDPR, for instance, encompasses data controllers without a presence in Europe if their processing activities occur within the EU. As a result, GDPR extends to entities outside the EU, including those in the US and non-EU countries, such as businesses, nonprofits, and universities, provided these entities offer goods or services to individuals in the EU or monitor the online behaviors of EU citizens. [60] Conversely, although HIPAA lacks explicit extraterritorial provisions akin to GDPR, it can potentially apply internationally. HIPAA stipulates that covered entities may engage business associates for handling PHI. In cases where a non-US entity is involved in handling, storing, or transmitting the PHI of US citizens or residents, it might be classified as a business associate of a US covered entity. Consequently, such an entity would be obligated to adhere to HIPAA regulations, even when operating abroad, thereby enabling the overseas application of HIPAA.

C. Individual Rights over Data

Since both regulations govern personal information of individuals, they both grant specific rights to individuals concerning their personal data. GDPR provides data subjects with the right to be informed, right of access to their data, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object, and right not to be subject to automated decision-making. [61] Similarly, HIPAA extends the right to individuals to request their health records, correct inaccurate information, understand the sharing of their health data and its recipients, object to specific disclosures, and determine preferred communication methods. Moreover, as an organizational obligation, entities subject to these laws are obligated to adequately inform individuals about their rights under each regulation and how their information is utilized.

D. Appointment of Compliance Officers

In the demonstration of compliance responsibilities, both GDPR and HIPAA necessitate organizations to designate individuals or entities as data protection officers and privacy officers, respectively. [62] These appointed personnel are tasked with developing, implementing, and enforcing policies and procedures required for privacy practices and compliance efforts. These officers must be employed by the organizations handling sensitive data, whether it's personal information or PHI.

E. Documentation and Record-keeping

These components are indispensable to compliance within these regulations. As compliance obligations, both regulations mandate organizations to uphold documentation and record-keeping practices. This is essential to demonstrate adherence to the regulations in their operations. This encompasses documenting the legal usage or disclosure of individual data, implementing protective measures for data, reporting breaches, implementing access controls, conducting audits, training employees, and determining retention periods for personal data and PHI. [63] Under both GDPR and HIPAA, organizations are also required to periodically review and update their documentation and record-keeping policies and procedures as outlined by these regulations.

F. Research

While GDPR allows sensitive personal data to be processed for scientific, historical, or statistical research, contingent upon appropriate technical and organizational safeguards to protect data subjects' rights and freedoms, [64] the Privacy Rule defines research as a systematic investigation aimed at developing or contributing to generalizable knowledge. [65] The Rule permits covered entities to use or disclose deidentified PHI for research purposes, subject to specific conditions. [66] The Rule outlines methods to appropriately inform individuals about the use and disclosure of their health information held by covered entities for research purposes, including the right to access such data.

G. Educating, Training, and Employee Awareness

These aspects are pivotal to compliance within GDPR and HIPAA. [67] These regulations mandate well-informed and trained employees who understand the principles, obligations, and rights contained within the laws. Employees must be educated and trained on handling personal data and PHI, responding to breaches and fulfilling notification requirements, obtaining consent for personal data and PHI usage and disclosure, understanding the rights of data owners, maintaining documentation and record-keeping, staying updated with policies, employing mechanisms to secure data appropriately, and comprehending penalties for non-compliance with these laws.

H. Reporting Security Breaches

Both regulations stipulate that organizations promptly notify affected individuals and regulatory authorities in the event of a data breach involving personal information or PHI. [68] These laws define the timeline for notifications to affected parties and relevant bodies, outline actions to be taken post-breach, and specify penalties for non-compliance. Under GDPR, breaches must be reported to the regulatory body within forty-two hours of identifying the breach. Under HIPAA, covered entities must report to HHS, affected individuals, and, in some cases, the media without unreasonable delay, but within sixty days of becoming aware of the breach.

I. Cross-Border Data Transfer

Both regulations establish limitations on transferring personal data or PHI beyond the regions they cover. Organizations must incorporate appropriate safeguards, such as standard contractual clauses or binding corporate rules, when transferring data across jurisdictional boundaries.

J. Penalties for Non-compliance/Violation

Sanctions are inherent in legal frameworks. In cases of non-compliance with man-made laws, penalties follow. Both GDPR and HIPAA outline penalties for non-compliance, which vary based on the severity of the violation. GDPR imposes administrative fines ranging from up to 10 million Euros or 2% of global turnover from the previous fiscal year, whichever is higher, for specific breaches, up to twenty million Euros or 4% of global turnover, for more serious violations. [69][70][71] HIPAA's penalty structure is tiered, with civil money penalties ranging from one hundred to fifty thousand dollars per violation, depending on the nature and severity of the breach. [72] The maximum annual penalty for HIPAA violations is one million five hundred dollars. [73] As of February 28, 2023, reported settlements or imposed civil money penalties under HIPAA amount to $134,828,772.00. [74] HIPAA also incorporates provisions for criminal penalties, including fines of up to two hundred and fifty thousand dollars and ten-year prison terms for intentional or wrongful PHI disclosure. Furthermore, the HITECH Act empowers state attorneys-general to initiate civil actions on behalf of state residents for violations of HIPAA Privacy and Security Rules. [75].

VI. DIFFERENCES BETWEEN THE GDPR AND HIPAA

Having highlighted the areas where the GDPR and HIPAA share some similarities, it is important to look at the material distinctions between both laws. The differences between the GDPR and HIPAA are identified as follows:

A. Scope

The GDPR regulates use and exchange of data; it defines data as information, especially facts or numbers, collected to be examined and considered and used to help decision-making or information in an electronic form that can be formed or used by a computer. [76]The GDPR seeks to protect personal data on a broader spectrum. Personal data can be defined as personal information relating to an identifiable natural person who can be identified either directly or indirectly, by reference to an identifier such as name, identification number, location data, online identifier, or to one or more specific to the physical, psychological, genetic, mental, economic, cultural, or, social identity of that person. [77] On a simpler note, personal information refers to data that can be employed to identify a natural person, which broadly embraces an individual’s name, home address, social security number, bank account details, telephone number, vehicle number plate, health records, biometric data, DNA, fingerprints, or any information that can differentiate the individual from another individual. The GDPR covers more than just health information, as a personal identifiable information. HIPAA, however, is narrower in scope as it provides safeguards to not all health data, but a specie of health information known as PHI only. The GDPR emphasizes on privacy by design and default, which is data protection through technology, and that there should be organizational and technical measures for protection of personal data. [78] HIPAA on the other hand focuses privacy and security of PHI.

B. Conceptualization

In describing the individuals, organizations, and activities they govern, the laws adopt special terms to mean similar concepts. The GDPR and HIPAA use different appellations to describe the persons whom they intend to protect their personal information. The GDPR refer to the owners of personally identifiable information as "data subjects," while HIPAA uses "individuals" to refer to as patients and consumers whose PHI are to be safeguarded. Furthermore, the GDPR uses the term "processing" to mean performing an action on personal data. Data processing means any operation or sets of operation which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [79] In essence, it means when personal information is collected and translated to meaningful or useable form. Personal data is lawfully processed if within any of the legal bases for data processing under the GDPR. [80]The HIPAA employs the phrase, "use and disclosure" to relate to any action performed on an individual's PHI in the US. Furthermore, GDPR regulates any organization maintain or handling personal data in the EU. GDPR recognizes data controllers and data processors. A data controller refers to a person who either alone, jointly with other persons or a statutory body determines the purposes for, and the way personal data is processed or is to be processed. [81] While HIPAA regulates covered entities and business associates who maintain or handle PHI. Lastly, the compliance officers as mandated by both laws for organizations handling personal data also bear distinct titles. The GDPR delineates these officers as "data protection officers," while HIPAA provides for both "privacy" and "security" officers.

C. The Dichotomy Between Consent and Authorization

Having regard for the specialness of health information, both laws require that before it can be processed or used/disclosed the consent or authorization of the owner of the information must be obtained. The GDPR defines consent as any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, which signifies agreement to the processing of personal data relating to him or her. [82]Health data is a sensitive personal information under the GDPR, which requires extra legal protection. Thus, to process health information under GDPR, the explicit consent of the data subject must be obtained, except where it falls within certain exceptions. [83] HIPAA provides that before a covered entity can use or disclose an individual's PHI, it must obtain the individual's prior written authorization or can only use or disclose where such falls under circumstances as the Privacy Rule may permit. Unlike the GDPR, the HIPAA does not define "authorization," it just sets it as a default rule. However, unlike consent under GDPR which may be given by means other than in writing, an authorization under HIPAA must be in writing, and must be satisfy some conditions, stating the specific use of the information to be used or disclosed, purpose of the disclosure and the expiration of the authorization.

Additionally, HIPAA has a "no conditioning" rule for the grant of an individual's authorization. This means HIPAA prohibits covered entitles from conditioning treatment, payment, enrollment, or eligibility on the grant of authorization by an individual. [81] GDPR on the other hand regards conditioning as a factor to determine the voluntariness of consent to process personal data. [85] Furthermore, HIPAA mandates that the individuals giving their prior written authorization for the use or disclosure of PHI must understand the importance of what they are signing. Thus, prohibiting the authorization from being combined with any other document. [86]Although this rule does not exist in absolute terms, as it has three exceptions, generally, HIPAA compels that an authorization must be presented separately to each individual for their signature. [87] GDPR, however, allows for the combination of written consent with any other declaration which also concerns other matters. [88] Essentially, what the GDPR requires is that the documents are presented in a way that is clearly distinguishable from other matters. From the foregoing, consent need not be separated, and can be combined with any other relevant matter.

Also, and importantly, both laws confer the rights of withdrawal or revocation of consent or authorization on data subjects or individuals to process or use/disclose their personal data or PHI. However, there is a sharp distinction in the operationalization of the rights in their different terms they are known as. The GDPR expressly permits a data subject to withdraw his or her consent to process his or her personal information, provided the personal information has not been already processed pursuant a prior given consent. [89] The GDPR provides that a data subject must be informed of his or her right to withdraw consent before giving the consent. The provision in the HIPAA Privacy Rule is, however, less stringent. The Rule provides that generally, an individual can revoke a prior given authorization insofar the revocation is in writing. [90] The Rule requires that the authorization itself contains a statement informing an individual of the right to revoke, the applicable exceptions to the right to revoke and how the individual can revoke a prior given authorization.

D. The Right to Erasure

This right is also known as the right to be forgotten or right to de-referencing. This right is typically a GDPR right, which allows a data subject to request a data controller the erasure of the personal data concerning him or her promptly under any the following circumstances:

1) Where the personal information are no longer necessary in for the purposes of their collection
2) Where the data subject withdraws consent on which the processing is based;
3) Where the data subject objects to the processing and there are no overriding legitimate grounds for processing
4) Here the personal information has been unlawfully processed;
5) Where the personal information must be erased for compliance with a legal obligation in the EU or any member State where the data controller is subject to; or
6) Where the personal data have been collected in relation to the offer of information society under the GDPR. [91]

This right was established in the cause celebre case of Google Spain SL, Google Inc, v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez. [92] In this case, Mr. Gonzalez petitioned that an offensive information about him be deleted for the inaccuracy on the respondents' platforms. The European Court of Justice ruled in his favor. Subsequently, in Google v. Commission Nationale de l'Informmatique et des libertes (CNIL), [93] The court held that the protection of personal information does not exist in absolute terms and must be considered vis-à-vis other fundamental rights as exercised in any society. In NT1 and NT2 v. Google LLC, [94] two businessmen were in the past convicted for criminal offences, their convictions later became spent under the Rehabilitation of Offenders Act. Both sued Google to delete the information about their convictions, as they had the right to be forgotten. The court, however, refused to make the delisting order, as it held the information remained relevant for the assessment of the men by members of the public. HIPAA, however, does not make provision for the right to erasure. As a matter of fact, it requires that covered entities to retain the records of an individual for six years from the time the documentation was created or was last in effect or was last in effect, whichever is later, even if the individual no longer interfaces with the covered entity. [95]

E. Compensation of Victims

The GDPR expressly entitles a data subject who has suffered a personal data breach from an organization to compensation for both material and non-material losses from. [96] The compensation can cover financial loss, emotional and psychological distress, or damage to reputation. A personal breach under the GDPR refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed. [97] An organization can be exempted from liability where it can prove it is not responsible for the breach. [98] HIPAA, however, has no express provision for the compensation of victims of a breach. On the other hand, HHS can impose monetary fines on subject entities that fail to comply with HIPAA, and it occasions harm on an individual. The affected individual can also initiate a civil action against a covered entity to recover damages for harm suffered because of HIPAA violation.

VII. CONCLUSIONS

his paper has traversed the realm of health data as a vital form of personal information in the digital age, where data breaches pose significant threats. In this context, the GDPR and HIPAA emerge as cornerstones, prioritizing the protection of health data amidst technological advancements. While differing in application, scope, approach, principles, and enforcement mechanisms, both legislations share a common goal: safeguarding health data and ensuring the privacy and security of this delicate form of personal information. Adhering to these regulations is not just a legal obligation; it fosters trust and confidence among data owners. As technology evolves, staying updated on regulatory changes and best practices is vital to prevent breaches and ensure compliance

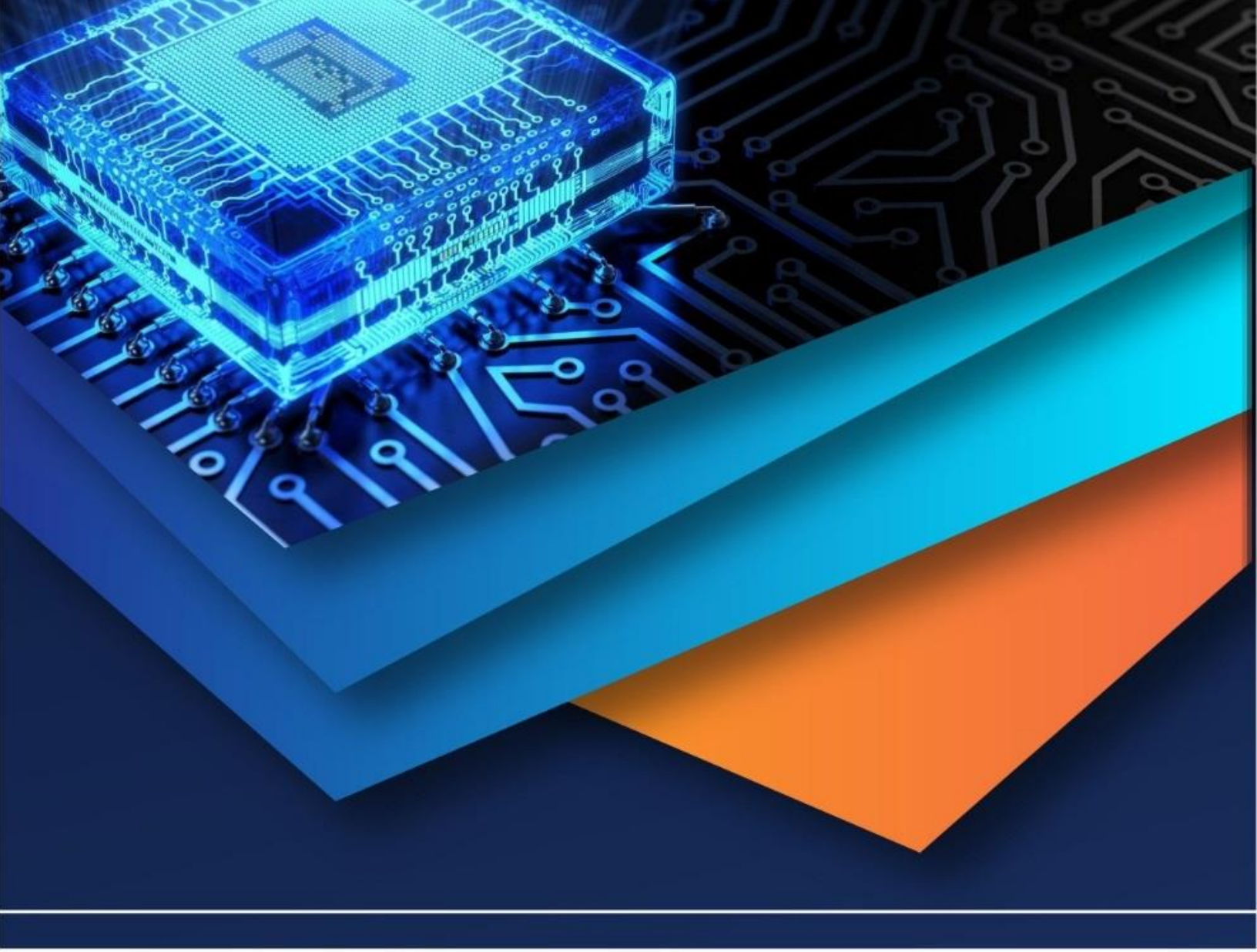
REFERENCES

[1] Israel Olawunmi is a Nigerian-trained legal practitioner, and currently, an LL.M candidate at the American University Washington College of Law, with concentration in Intellectual Property and Technology Law. He can be reached at olawunmiisrael10@gmail.com.
[2] Israel Olawunmi and Chukwumezie Charles Emejuo, An Examination of the Legal Framework for Data Privacy and Protection in Nigeria, 1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id4058446 accessed March 23, 2023.
[3] Purvi Nema & Riya Sinha, Privacy and Security Concerns in Electronic Health Records- A Comparative Study Between India and USA, [2020] (1) (1) Journal of Law and Legal Studies, 6 https://hcommons.org/deposits/objects/hc:43076/datastreams/CONTENT/content accessed March 23, 2023
[4] Brooke Bennett et al, AHLA Health Care Compliance Legal Issues Manual (5th edn, AHLA, 2019), 448
[5] George. J. Annas, HIPAA Regulations- A New Era of Medical Privacy, [2003] (348) The New England Journal of Medicine, 1486 https://scholarship.law.bu.edu/faculty_scholarship/1283/ accessed March 23, 2023

[6] Daniel J. Solove & Paul M. Schwartz, An Overview of Privacy Laws in 2022, (Chapter 1 of Privacy Law Fundamentals, 6th edn, IAPP, 2022), GWU Law School Public Law Research Paper No. 2022-26, 36 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4072205 accessed March 23, 2023
[7] Ibid
[8] Dana Vioeranu, The Origins of Privacy and How It Became a Human Right, https://www.cyberghostvpn.com/en_US/privacyhub/the-origins-of-privacy-and-how-it-becae-a-human-right/ accessed \March 28, 2023
[9] Kirk. J. Nahra, Privacy Law and the First-Year Law School Curriculum, http://greenbag.org/v23n1/v23n1_articles_nahra.pdf , 23, accessed March 28, 2023
[10] Samuel. D. Warren and Louis. D. Brandeis, The Right to Privacy, [1890] (IV) (5) Harvard Law Review, 1 http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html accessed March 28, 2023
[11] Article 12 UDHR
[12] Article 8 Charter of Fundamental Rights of the European Union.
[13] James Grimmelmann, Internet Law: Cases & Problems, (12th edn, Semaphore Press, 2022) 311
[14] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Data Regulation) COM /2012/011 Final-2012/0011 (COD) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012PC0011 accessed March 28, 2023
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL accessed March 28, 2023
[16] Matt Burgess, What is GDPR? The Summary Guide to GDPR Compliance in the UK, https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 accessed March 28, 2023
[17] Article 3.1 GDPR
[18] Article 3.2 GDPR. The US equivalent of the GDPR is the California Consumer Privacy Act, applicable in California.
[19] Article 4 (7) GDPR.
[20] Article 9 (1) GDPR.
[21] Article 5(1) GDPR
[22] Article 6(1) GDPR
[23] Chapter 3 GDPR, art. 12-23
[24] Judith Havemann, President Signs Insurance Portability Bill Into Law, The Washington Post, 1996, https://www.washingtonpost.com/archive/politics/1996/08/22/president-signs-insurance-portability-bill-into-law/46ea70fe-50ee-4c17-8209-3f99045b123e/ accessed March 28, 2023
[25] The duo had prior sponsored the Health Insurance Reform Act 1995, which is commonly touted as a forerunner of HIPAA. However, it was not passed- One of the major reasons being that it omitted to account for the cost that may be shouldered by the healthcare insurance operators that it would apply to.
[26] Clinton Foundation, Health Insurance and Portability and Accountability Act (HIPAA) at 25- The Lasting Health Privacy Protections of the Clinton Administration, (2021) https://medium.com/@ClintonFdn/health-insurance-portability-and-accountability-act-hipaa-at-25-the-lasting-health-privacy-b1809a15af21 accessed March 28, 2023. A. job lock is a situation in which a plan member is compelled to stay on a job to prevent losing health plan benefits.
[27] The HIPAA Guide, History of HIPAA, https://www.hipaaguide.net/history-of-hipaa/ accessed March 28, 2023
[28] Pension Benefit Guaranty Corporation, President Ford Signing ERISA of 1974, https://www.pbgc.gov/about/who-we-are/pg/president-ford-signing-erisa-of-1974 accessed March 28, 2023
[29] The HIPAA Guide, op cit. A preexisting condition relates to a health condition that was present before the date of enrollment for coverage, whether any medical advice, diagnosis, care, or treatment was recommended or received before the enrollment date.
[30] The HIPAA Journal, HIPAA History, https://www.hipaajournal.com/hipaa-history/ accessed March 28, 2023. Sections 201-205 HIPAA. Also, see: Preamble to HIPAA.
[31] 45 CFR § 160.103. A covered entity will be discussed in the latter part of this work.
[32] §1172(a)(1) HIPAA.
[33] A health plan is an individual or group that provides or pay for the cost of medical care. A health plan does not have to transmit health information in electronic form to be categorized as a covered entity, it only needs to carry on the business of providing or paying for the cost of medical care. Typically, a health plan includes health insurance companies, health maintenance organizations (HMOs), company health plans and government health care plans such as Medicare, Medicaid, the Children's Health Insurance Program, Federal Employee Health Benefit Program, TRICARE/CHAMPUS, and military and veteran health care programs. A health plan excludes coverage only for accidents, disability income insurance or any combination, coverage issued as supplement to liability insurance (including general liability insurance and automobile insurance), workers' compensation or similar insurance, coverage for on-site medical clinics, and other similar insurance coverage under which benefits for medical care are secondary or incidental to other insurance benefits, even though they may provide payment for medical care cost.
[34] A health care clearinghouse is an entity that processes or facilitates non-standard data elements of health information it receives from another entity into a standard format or vice-versa. Examples include billing services and community health care system for managing health status. An internet service provider (ISP) or telecommunication company supplying transmission for health plans and health providers, is not a covered entity under HIPAA if it solely acts as a transmission conduit or solely provides connectivity. A Health Information Organization can, however, be treated as a business associate.
[35] Health care providers include medical doctors, clinics, psychologists, dentists, home health agencies, hospices, chiropractors, comprehensive outpatient rehabilitation facilities, nursing homes, pharmacies, and suppliers of ancillary services, if they transmit health data in electronic form in a transaction regulated by HIPAA. A school health center albeit is a health care provider, it is not covered under HIPAA but under the Family Educational Rights and Privacy Act (FERPA). Apple watch/Fitbit are no health care providers covered by HIPAA. Drug manufacturers are also not covered entities covered by HIPAA. An employer is a covered entity under HIPAA to the extent of the health care services to its employees.
[36] Section 1173 (a)(1) HIPAA; 45 CFR § 160.103.
[37] Pub. L. 108-173, 42 U.S.C. § 1395w-141(h)(6)(A). This statute also extends the application of the HIPAA Privacy Rule to covered entities.
[38] Sections 261-264 of HIPAA mandates the Secretary of HHS to introduce these rules.

[39] 45 CFR § 160.103
[40] 45 CFR § 160.103. The HIPAA Final Rule provides that a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a covered entity and routinely requires access to the PHI is also within the definition o f a business associate.
[41] 45 CFR § 164.512 (a)(2)
[42] 45 CFR § 164.512 (a)(1)
[43] It is important to develop standard rules on how organizations can determine what is the minimum necessary information to be disclosed. Employees also must be trained to evaluate and appreciate these rules to know how to always apply them appropriately in all cases.
[44] HHS.gov, Summary of the HIPAA Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html accessed April 9, 2023
[45] 45 CFR § 160.103, 164.302
[46] 78 Fed. Reg. 5566
[47] 45 CFR § 164.306, (b)(2)
[48] 45 CFR § 164.304,
[49] 45 CFR § 164.308, (a)(1)(i)
[50] OCR issued Guidance on Risk Analysis Requirements under the Security Rule, available at https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es
[51] 45 CFR § 164.310
[52] 45 CFR § 164.312
[53] 45 CFR § 164.400-414. The Federal Trade Commission (FTC) has similar breach notification provisions that apply to vendors of PHI and their third-party service providers, made pursuant to section 13407 HITECH Act.
[54] 45 CFR § 164.402(2)
[55] Article 4 (1) GDPR
[56] Article 5(1) GDPR
[57] There are, however, some instances where obtaining authorization would unnecessary under HIPAA.
[58] Article 5(1) GDPR; § 164.308, (a)(1)(i)
[59] Israel Olawunmi, The African Continental Free Trade Area Agreement Vis-à-vis Its Data Protection Concerns, (SSRN, 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3960042&download=yes , 1 accessed April 11, 2023
[60] Article 3.2 GDPR. The US equivalent of the GDPR is the California Consumer Privacy Act, applicable in California.
[61] Chapter 3 GDPR, art. 12-23
[62] Article 37 GDPR; 45 CFR § 164.530(a)(1). HIPAA also provides for the designation of a security officer.
[63] Notably, although the GDPR provides for retention of documents as they affect personal data, HIPPA provides that covered entities and business associates must keep records for at least six years from the time it was created.
[64] Article 5(e) GDPR
[65] 45 CFR § 164.501
[66] 45 CFR § 164.502(2); 45 CFR § 164.514(a)-(c)
[67] Article 39 GDPR
[68] Articles 33-34 GDPR
[69] Article 83(4) GDPR
[70] Article 83(5) GDPR
[71] Article 83(6) GDPR
[72] 45 CFR § 160.404
[73] id
[74] HHS.gov, Enforcement Highlights, (HHS, 2023) https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html accessed April 15, 2023
[75] 42 U.S.C. § 1320(d)(1)
[76] Cambridge Online Dictionary, https://dictionary.cambridge.org/dictionary/english/data accessed April 15, 2023
[77] Article 4 (1) GDPR
[78] Article 25 GDPR
[79] Article 4(2) GDPR
[80] Article 6 GDPR
[81] Article 4 (7) GDPR.
[82] Article 4(11) GDPR
[83] Article 9 GDPR
[84] 45 CFR § 164.508(b)(4) provides three exceptions, however.
[85] Article 7(4) GDPR
[86] 45 CFR § 164.508(b)(3)
[87] 45 CFR § 164.508(b)(3)(i)-(iii)
[88] Article 7(2) GDPR
[89] Article 7(3) GDPR
[90] 45 CFR § 164.508(b)(5)
[91] Article 17 GDPR
[92] C-131/12, June 25, 2013 (ECJ)
[93] C-507/17

[94] [2018] EWHC 799 (QB)
[95] 45 CFR § 164.530(j)(2)
[96] Article 82 (1) GDPR
[97] Article 4(12) GDPR
[98] Article 82 (3) GDPR



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)