A review into the evolution of HIPAA in response to evolving technological environments

Abhishek P. Patil[1], Neelika Chakrabarti [2]

[1]School of Technology Management and Engineering, NMIMS University, Mumbai, INDIA;
abhishekpatil.nmims@gmail.com

[2] School of Technology Management and Engineering, NMIMS University, Mumbai, INDIA;
neelikachakrabarti.nmims@gmail.com

Abstract

The Health Insurance Portability and Accountability Act of 1996 was brought in to serve as a legislation that could essentially assist in reorganizing the flow of healthcare information, prescribing how sensitive medical data stored with healthcare/insurance firms should be protected from stealing and tampering. It has served as a pioneer in the world of privacy in healthcare and set one of the earliest benchmarks for any legal instruments regarding the storing and dissemination of medical information in the form of electronic health records. The HITECH act of 2009 and the HIPAA omnibus rule of 2013 further cemented the use of standardized frameworks which can help control, reduce and track any possible breaches of confidentiality and integrity of such personal information. This paper explores the content, reasoning, and timeline of the HIPAA act and the impact it creates on the health information technology sector. It also explains the challenges that are faced in the implementation of the policy and gives a holistic perspective of the rights and responsibilities of each stakeholder involved.

Keywords: HIPAA, Data Privacy, Healthcare, Insurance, Insuritech, EHR, Policy, Medical Data

1. Introduction

The Health Insurance Portability and Accountability Act of 1996 was brought in to serve as a legislation that could essentially assist in reorganizing the flow of healthcare information, prescribing how sensitive medical data stored with healthcare/insurance firms should be protected from stealing and tampering. It has served as a pioneer in the world of privacy in healthcare and set one of the earliest benchmarks for any legal instruments regarding the storing and dissemination of medical information in the form of electronic health records.

The HITECH act of 2009 and the HIPAA omnibus rule of 2013 further cemented the use of standardized frameworks which can help control, reduce and track any possible breaches of confidentiality and integrity of such personal information. This paper explores the content, reasoning, and timeline of the HIPAA act and the impact it creates on the health information technology sector. It also explains the challenges that are faced in the

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

implementation of the policy and gives a holistic perspective of the rights and responsibilities of each stakeholder involved.

The Health Insurance Portability and Accountability Act consists of Standardized Electronic Data Interchange transactions & codes for involved entities, standards for security data systems, privacy protection for individual health information and standard national identifiers for healthcare [1].

HIPAA ensured that individual healthcare services plans are available, portable and inexhaustible, and it sets the principles and the strategies for how clinical information is shared over the U.S. wellbeing framework so as to forestall extortion [2][3]

The goals of HIPAA can widely be described as:

- To make the law easier for people to keep insurance.
- To standardize the policy framework regarding Electronic Health Record(EHR) privacy and ease the evolution and necessary adaptation of laws as the technology around the storage of these develops
- To enable development of a network infrastructure that could be used by stakeholders in multiple industries like insurance, healthcare, pharmaceuticals etc. to avoid duplication of effort and resources through a unified systematic approach
- To protect the confidentiality and integrity of healthcare information and any Personally Identifiable Information (PII) that might be deemed sensitive by the patients and intermediary entities
- To minimize administrative costs incurred in the healthcare industry due to legacy record maintenance systems while keeping the trade-off against security and prioritization of privacy in mind

The enforcement of all these regulations has caused certain applications of medical data records to reevaluate and re-engineer scope of operations. Not only did this have an impact on practicing physicians, but also researchers and insurance providers.

Researchers' old methodology of using open source data to perform analysis and identifying patterns has become increasingly hard due to the inability to isolate the patient information from the patient identity.

It's inherently complex nature has raised concerns multiple times and there have been consistent measures taken by the Department of Health and Human Services to ease administration and ensure compliance, including but not limited to the Administrative Simplification Compliance Act.

2. A brief overview of the timeline of HIPAA and its associated acts

Figure 1 The linear timeline of important events since the HIPAA was instituted and when its associated acts were brought into action. [2].

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

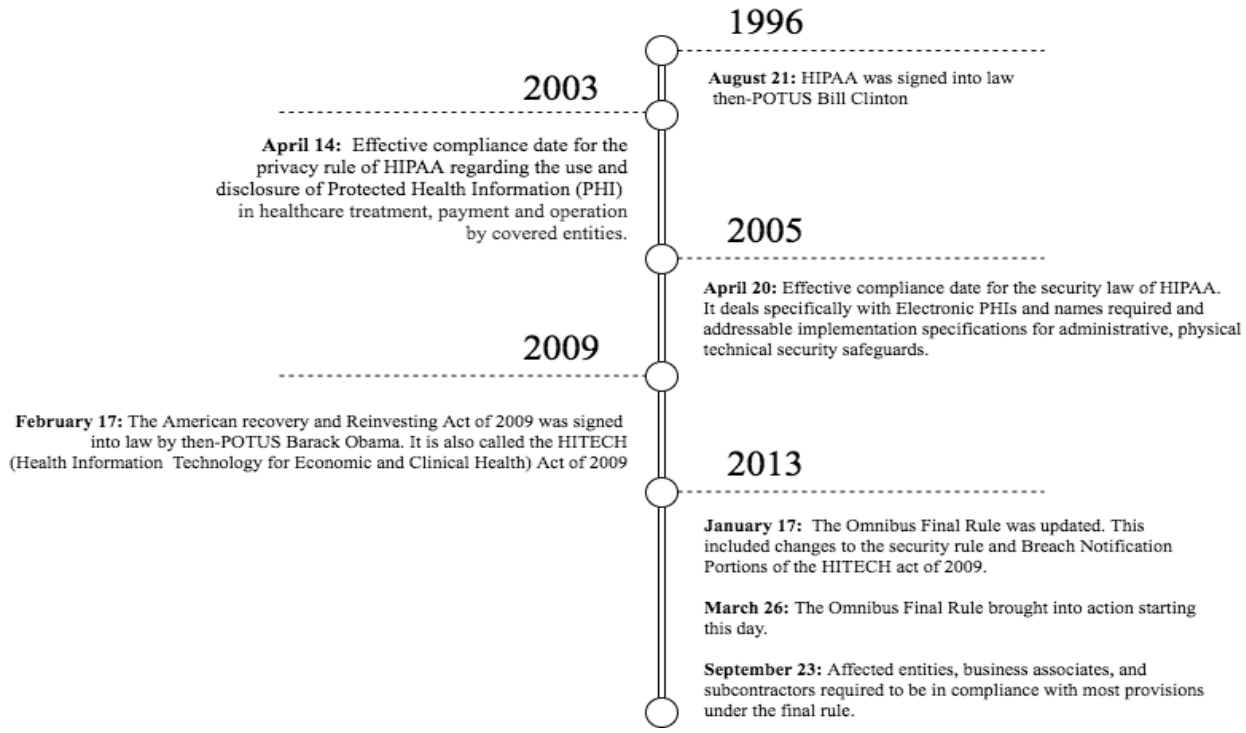

Figure 1: Timeline of HIPAA and relevant acts

3. Entities covered under HIPAA

The entities covered under HIPAA can widely be categorized into three categories, two of which (Healthcare Service providers and Health Plan Providers) are listed and compared in Table 1 below:

Table 1: Characteristics of healthcare service providers and health plan providers

Healthcare Service Providers	**Health Plan Providers**
This includes: ● Doctors ● Clinical Staff ● Therapists/Psychologists ● Dentists ● Chiropractors ● Nursing Homes ● Pharmacies	This includes: ● Insurance Partners ● Govt. programs included in HMOs

Additionally, the act also includes Healthcare clearinghouses. These are "public or private entities, including billing

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020
DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

services, repricing companies, or community health information systems, which process non-standard data or transactions received from one entity into standard transactions or data elements, or vice versa," as described by the Department of Health and Human Services [3].

4. Information protected under this act

HIPAA laws ensure all independently recognizable healthcare data that is in the possession of and operated upon by entities mentioned in Table 1. As indicated by Department of Healthcare and Human Service's Officer for Civil rights upholds a total of 18 data record types that make wellbeing data by and by recognizable. At the point when these information components are remembered for an informational collection, the data is viewed as ensured wellbeing data and subject to the prerequisites of the HIPAA Privacy, Security and Breach Notification Rules [4][5].

The following information is protected under HIPAA law:[12]

1. Names
2. Addresses (including subdivisions smaller than state such as street, city, county, and zip code)
3. Dates (except years) directly related to an individual, such as birthdays, admission/discharge dates, death dates, and exact ages of individuals older than 89
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate and license numbers
12. Vehicle identifiers
13. Device identifiers and serial numbers
14. Website URLs
15. IP addresses
16. Biometric identifiers, including fingerprints, voice prints, iris and retina scans
17. Full-face photos and other photos that could allow a patient to be identified
18. Any other unique identifying numbers, characteristics, or codes

Some other aspects to look at include: -

- *"Individually identifiable health information* is information, including demographic data, that relates to: the person's past, present or future physical or psychological wellness or condition, the arrangement of medicinal services to the individual, or the past, present, or future installment for the arrangement of human services to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual"[6].
- "The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the **Family Educational Rights and Privacy Act, 20 U.S.C. §1232g."**

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

- De-Identified Health Information. "There are no limitations on the utilization or revelation of de-recognized wellbeing data. De-recognized wellbeing data neither distinguishes nor gives a sensible premise to distinguish a person. There are two different ways to de-recognize data; either: (1) a proper assurance by a certified analyst; or (2) the evacuation of determined identifiers of the individual and of the person's family members, family individuals, and businesses is required, and is satisfactory just if the secured substance has no genuine information that the rest of the data could be utilized to distinguish the person."
- Re-Identified Health information. "A re-identification, also known in the literature as an identity disclosure, occurs when an attacker can make a likely match between a de-identified record and the corresponding record in any primary identified dataset" [7].

5. Patient rights under HIPAA

One of the primary purposes of HIPAA was to make medical record maintenance more resource efficient while also maintaining security and privacy of the patients in question. The paradigm shift in the systems brought in new challenges which required rights which were assumed to be indivisible from the previous systems because of the lack of an electronic infrastructure. Making the rights of the patient an important section to be given thought to [8].

HIPAA grants individuals whose records are maintained in EHR system the following rights:

1. **Right to Access**: This is the right to ask for and observe a copy of medical information used to decide the status and future of the treatment. This can include medical and billing records. "Access" means that the patient may review, inspect, and obtain a copy of your health information. This excludes psychotherapy notes as they are used for treatment purposes and access to that information could tamper with the treatment.
2. **Right to Accounting of Disclosures**: This is the right to request an a list, of all disclosures made about the patient's health information. The list of disclosures includes: The date of the disclosure, the name of the entity to whom the information was disclosed, and, if known, the communication address or telephonic details, a brief description of the medical information that was disclosed, and a brief summary of the intent for which the disclosure was made.
3. **Right to Request for Amendment**: The patient may request for amendment if the medical or health information is incorrect or incomplete. This request for an amendment can be made if the information is kept by or for the institution. The request to amend can be denied if the person/entity that created the information record or indefinitely not available to make the amendment, or is not a part of the information that the patient would be allowed to inspect and copy, or if the information is accurate and complete already.
4. **Right to Request Confidential Communications**: Patients might want to receive communication regarding their EHR in private and while maintaining confidentiality. They can request to use alternative methods or locations to communicate about the EHRs so that they receive the communication only in desired manners, desired environment and in front of the desired company.
5. **Right to Request for Restrictions:** This is the right to request a restriction or limitation on the medical information used or disclosed about the patient for treatment, healthcare functions or payments. The patient can ask to limit the medical information that is disclosed to individuals (friends or family members) who are involved in the care or payment of treatments required. This request can be rejected, but if it agreed it is complied with until emergency situations call for a breach.
6. **Right to Restrict Disclosure to Health Plan**: This is the right to restrict information about previous medical records to the Health plan provider provided it is not a malicious attempt to hide previous medical history that could tamper with the treatment and calculations of the payments due towards the health plan into the future.
7. **Right to Complain for Privacy Rights Violation:** The patient has the right to complain if they notice that their information has been used or disclosed inappropriately and for purposes other than what it was intended for.

6. Compliance and enforcement under HIPAA

Risk assessment and management is a key consideration for HIPAA IT compliance. One approach to help guarantee dangers are distinguished and fitting controls executed as a component of the HIPAA IT compliance program is to

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

receive the NIST Cybersecurity Framework. The NIST Cybersecurity Framework will assist you with preventing information breaches, and identify and react to assaults in a HIPAA consistent way when assaults do happen [9].

HIPAA IT compliance concerns all frameworks that are utilized to transmit, get, store, or modify electronic ensured wellbeing data. Checking ePHI logs routinely and directing normal reviews is an absolute necessity to look after consistency. Potential slips by in security because of the utilization of individual cell phones in the work environment can be dispensed with by the utilization of a protected informing arrangement. Secure informing arrangements permit approved workforce to convey PH. Messages containing PHI that are sent past an inward firewalled served ought to be encoded.

As clinical records can pull in a higher selling cost on the black market than charge card subtleties, guards ought to be set up to forestall phishing assaults and the incidental downloading of malware.

Following are certain modifications to HIPAA that are in the pipeline-

- Restitution payments to individuals who's PHI had been disclosed in a breach of HIPAA.
- The removal of the requirement to store forms acknowledging receipt of Privacy Notices.
- Clarification of what are considered as "good faith" disclosures when a patient is incapacitated. (cite HIPAA journal)

7. HIPAA vis-à-vis GDPR

The General Data Protection Regulation (GDPR) of the European Union (EU) came in as a replacement to the country by-country laws under the 1995 Data Protection Directive (DPD).[11] The GDPR and HIPAA share similarities in terms of data privacy objectives and definitions. However, there exist certain notable differences in terms of provisions and coverage.

Table 2: certain notable differences in terms of provisions and coverage.

GDPR	**HIPAA**
GDPR focuses on protecting the PII (personally identifiable information) of EU citizens.	HIPAA focuses on business entities and organizations dealing with PHI (public health information) within USA.
Includes the Right to be Forgotten under which citizens may request a complete deletion of their data.	No such provision exists.
Explicit patient consent is required to process any request.	PHI disclosure is allowed under special circumstances without patient's consent.
A data breach has to be reported within a 72 hour window	A data breach has to be reported within 60 days if it is a large breach (500+ cases) and it has to be reported before the annual reporting day for smaller breaches.
Permits data processing and sharing with not for profit organizations if it involves on the patient's family.	No such rule exists.

8. HITECH Act

The cost of providing healthcare is increasing now more than ever due to the hike in the number of diseases and ease of accessibility through their sources. If they continue to increase even at the present growth rate which is considerably steady then funds like Children's Health Insurance Program, Medicare, Medicaid etc. are expected to take up 10% of GDP in 2035, relative to 5.5% 5 today. The shift from manual bookkeeping to EHR systems and the consequent automation of medical recordkeeping would not only enhance the quality of service but also the cost effectiveness of services in the medical industry. The American Recovery and Reinvestment Act along with the HITECH act was brought into power in the year 2009 and was expected to act as a stimulus to move systems across the nation of USA to adopt EHR systems. The framework calls for a shift from physician autonomy to large scale data sharing. This allows evidence-based diagnosis approaches and the use of other best practices in the healthcare industry.

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

HITECH act provided a lot of incentives to medical healthcare providers for the immediate adoption and appropriate use of EHR systems. It also has significant fines and penalties to ensure enforcement. These penalties could come as reduced reimbursements for patient services as the reimbursements are centralized.

HITECH act also builds up on the privacy and security pillars of the HIPAA act. It prohibits unauthorized sale of medical records except for in cases of academic research and public health. It calls for the need to maintain an audit trail of people who have access to information on each record.

The HITECH act uses a level system which increases the pecuniary penalties for non-compliance. This enforcement mechanism imposes fines that vary from $100 to $50000 per violation. The maximum fine that can be imposed is for willful misconduct, at around $1,500,000. In a nutshell, the HITECH act builds on HIPAA Privacy and Security rules and mandates adoption of EHR systems, making manual bookkeeping nonexistent.

Table 3: Administrative Safeguard

Administrative Safeguards; Standard Sections Implementation Specification		
(R) - Required, (A) – Addressable		
Security Management Process	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R
Assigned Security Responsibility		R
Workforce Security	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A
Information Access Management	Isolating Healthcare Clearinghouse Function	R
	Access Authorization	A
	Access Establishment and Modification	A
Security Awareness and Training	Security Reminders	A
	Protection from Malicious Software	A
	Log-In Monitoring	A
	Password Management	A
Security Incident Procedures	Response and Reporting	R
Contingency Plan	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

	Testing and Revision Procedure	A
	Applications and Data Criticality Analysis	A
Evaluation	Response and Reporting	R
Business Associate Contracts and Other Arrangement	Written contract or other arrangement	R

Table 4: Physical Safeguards

Physical Safeguards; Standard Sections Implementation Specification (R) - Required, (A) – Addressable		
Workstation Use		R
Workstation Security		R
Device and Media Controls	Disposal	R
	Media Re-Use	R
Assigned Security Responsibility	Accountability	A
Workforce Security	Data Backup and Storage	A

Table 5: Technical Safeguards

Technical Safeguards; Standard Sections Implementation Specification (R) - Required, (A) – Addressable		
Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A
Audit Controls		R
Integrity	Mechanism to Authenticate ePHI	A
Person or Entity Authentication		R
Transmission Security	Integrity Controls	A
	Encryption	A

9. Challenges for HIPAA in the Digital Age

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020
DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

During a time of fitness tracking applications and GPS-followed, shareable information on everything from a person's day by day step check to their normal pulse, prescriptions, sensitivities and so on there are new difficulties for maintaining gauges for upholding standards in storing and protecting personal clinical data.Integration with other laws is a major challenge. Privacy laws that have come in later in other jurisdictions cover the same arrangements as the HIPAA itself. Firms that operate in multiple jurisdictions including the US need to assess the similarities and contradictions between the two legal requirements before operatting. This has been the case with companies acting out of the European Union (GDPR) and California (the CCPA).

HIPAA needs amendments that would help make data less susceptible to privacy breach risks when stored on the cloud. While HIPAA does cover electronic health records and their distribution of communication networks, the lack of direct active management by the user and the adoption of service oriented architecture necessitate specific frameworks that can adapt with the exponentially evolving cloud technology.

Figure 2 highlights the challenges faced by HIPAA in any possible modular changes to make it compatible with technological advancements

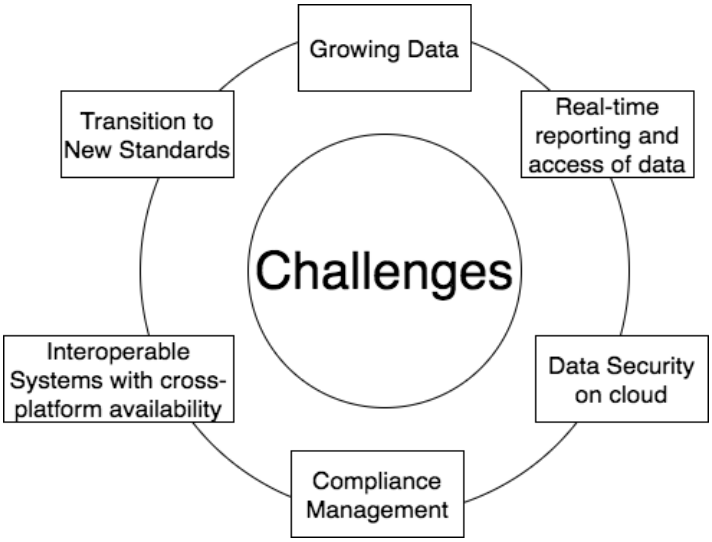

Figure 2: Challenges faced by HIPAA

In 2009, **the Health Information Technology for Economic and Clinical Health Act (HITECH)** expanded HIPAA security and security protections. The HITECH Act was sanctioned as a major aspect of the **American Recovery and Reinvestment Act of 2009** so as to advance the utilization of healthcare data innovation.
Presently, however, insurance agencies and human services suppliers are dependent upon laws that require compliance with HIPAA's security and security assurances, organizations like Fitbit and Apple aren't held to comparable guidelines [10].

10. Conclusion

HIPAA required the Secretary to give security guidelines administering individually identifiable health information, if Congress didn't authorize protection enactment inside three years of the section of HIPAA.
HIPAA and HITECH have played a fundamental role in regulating the privacy concerns related to storing medical data electronically and how it should be shared with entities covered in table 1. Both the regulations together have a very wide extent that influences spheres that would no directly communicate with each other in an EHR-less world. It has to function symbiotically with the multitude of legal guideline concerning data privacy in a general context. This frequently calls for periodic reviews to ensure that the compliance does not override

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020
DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

any other existing legislations, especially when the domain has ambiguity on how to deal with PII. Privacy legislation is constantly evolving as technological advances and societal perspectives change towards how the EHR systems are integrated into daily lifestyle.

Table 6: Technical Safeguards

Abbreviation	Meaning
HIPAA	Health Insurance Portability and Accountability Act
EHR	Electronic Health Record
HMO	Health maintenance organization
HITECH	Health Information Technology for Economic and Clinical Health Act
PII	Personally Identifiable Information
PHI	Public Health Information
GDPR	General Data Protection Regulation
GPS	Global Postioning System
EU	European Union
DPD	Data Protection Directive
NIST	National Institute of Standards and Technology
CCPA	California Consumer Privacy Act
HHS	Health and Human Services

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

1. Kwon, Juhee, and M. Eric Johnson. "Protecting patient data-the economic perspective of healthcare security." *IEEE Security & Privacy* 13, no. 5 (2015): 90-95.
2. Piliouras, Teresa, Xin Tian, Dhaval Desai, Avani Patel, Dhara Shah, Yang Su, Pui Lam Yu, and Nadia Sultana. "Impacts of legislation on electronic health records systems and security implementation." In *2012 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pp. 1-7. IEEE, 2012.

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**

3. Hu, Jiankun, Hsiao-Hwa Chen, and Ting-Wei Hou. "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations." *Computer Standards & Interfaces* 32, no. 5-6 (2010): 274-280.
4. Ness, Roberta B., and Joint Policy Committee. "Influence of the HIPAA privacy rule on health research." *Jama* 298, no. 18 (2007): 2164-2170.
5. Benitez, Kathleen, and Bradley Malin. "Evaluating re-identification risks with respect to the HIPAA privacy rule." *Journal of the American Medical Informatics Association* 17, no. 2 (2010): 169-177.
6. Lee, Wei-Bin, and Chien-Ding Lee. "A cryptographic key management solution for HIPAA privacy/security regulations." *IEEE Transactions on Information Technology in Biomedicine* 12, no. 1 (2008): 34-41.
7. Annas, George J. "HIPAA regulations—a new era of medical-record privacy?." (2003): 1486-1490.
8. Gostin, Lawrence O., and Sharyl Nass. "Reforming the HIPAA privacy rule: safeguarding privacy and promoting research." *Jama* 301, no. 13 (2009): 1373-1375.
9. Murray, Tracey L., Mona Calhoun, and Nayna C. Philipsen. "Privacy, confidentiality, HIPAA, and HITECH: implications for the health care practitioner." *The Journal for Nurse Practitioners* 7, no. 9 (2011): 747-752.
10. Kempfert, Amy E., and Benjamin D. Reed. "Health care reform in the United States: HITECH Act and HIPAA privacy, security, and enforcement issues." *FDCC Quarterly* 61, no. 3 (2011): 240.
11. Koeninger, Kelly, Robinson Bradshaw, P. A. Hinson, and John Conley. "International Health Data: How HIPAA Interacts with the EU GDPR."
12. Health Insurance Portability and Accountability Act.

Received: May 27, 2020 Revised: July 21, 2020 Accepted: August 24, 2020

DOI: 10.5281/zenodo.4014219 **Special issue on Research and Innovations in Data Protection and Privacy in Healthcare (RIDAPPH)**