Scientific Research Publishing

Journal of Information Security, 2024, 15, 232-244
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

United States Healthcare Data Breaches: Insights for NIST SP 800-66 Revision 2 from a Review of the NIST SP 800-66 Revision 1

Mohammed Mohammed Raoof

Center for Information Systems & Technology, Claremont Graduate University, Claremont, USA
Email: mohammedraoofphd@gmail.com

How to cite this paper: Mohammed Raoof, M. (2024) United States Healthcare Data Breaches: Insights for NIST SP 800-66 Revision 2 from a Review of the NIST SP 800-66 Revision 1. *Journal of Information Security*, **15**, 232-244.
https://doi.org/10.4236/jis.2024.152014

Received: March 30, 2024
Accepted: April 26, 2024
Published: April 29, 2024

Abstract

Healthcare security and privacy breaches are occurring in the United States (US), and increased substantially during the pandemic. This paper reviews the National Institute of Standards and Technology (NIST) publication base as an effective solution. The NIST Special Publication 800-66 Revision 1 was an essential standard in US healthcare, which was withdrawn in February 2024 and superseded by SP 800-66 Revision 2. This review investigates the academic papers concerning the application of the NIST SP 800-66 Revision 1 standard in the US healthcare literature. A systematic review method was used in this study to determine current knowledge gaps of the SP 800-66 Revision 1. Some limitations were employed in the search to enforce validity. A total of eleven articles were found eligible for the study. Consequently, this study suggests the necessity for additional academic papers pertaining to SP 800-66 Revision 2 in the US healthcare literature. In turn, it will enhance awareness of safeguarding electronic protected health information (ePHI), help to mitigate potential future risks, and eventually reduce breaches.

Keywords

SP 800-66 Revision 1, SP 800-66 Revision 2, HIPAA Compliance, Security Breaches, Risk Management Framework (RMF), Internet of Things (IoT), Artificial Intelligence (AI)

1. Introduction

In view of various facets of the situations, circumstances, and technology abuse, healthcare data breaches have remained elevated in the United States (US). A recent study [1] stated that the US healthcare industry observed an increment of

25 percent in successful cybersecurity attacks during the COVID-19 pandemic. Technology abuse is exemplified by ransomware and many other technological techniques attacks; Another study [2] fueled the growth of data breaches in US healthcare delivery organizations. Moreover, further study [3] noted that US healthcare breaches frequently occur at extraordinary rates, resulting in financial loss, reputation loss, and the possibility of losing the business.

As one of the essential solutions, the National Institute of Standards and Technology (NIST) published a wide variety of publications on information security; one of those publications was the 2008 NIST Special Publication SP 800-66 Revision 1, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" [4].

As stated in NIST's introduction to HIPAA security implementation [4]: "This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. The publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. It is also designed to direct readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule." We conclude that SP 800-66 Revision 1 targets readers' awareness of US healthcare security. Moreover, under the HIPAA Security Rules, covered entities are required to evaluate risks and vulnerabilities in their environments and to implement security controls to address those risks and vulnerabilities [4].

According to the Department of Health and Human Services (HHS), the covered entity is any one of the following displayed in **Table 1**. [5]

The SP 800-66 Revision 1 standard has a Risk Management Framework (RMF). The NIST RMF, "provides the covered entity with a disciplined, structured, extensible, and repeatable process for achieving risk-based protection related to the operation and use of information systems and the protection of" Electronic Protected Health Information (EPHI) [4].

Table 1. The types of covered entities.

A Health Care Provider	This includes providers such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies, but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.
A Health Plan	This includes Health insurance companies, Health Maintenance Organizations (HMOs), company health plans, and Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs.
A Health Care Clearinghouse	This includes entities that process nonstandard health information they receive from another entity into a standard (*i.e.*, standard electronic format or data content), or vice versa.

Figure 1 illustrates the NIST Risk Management Framework (RMF). As mentioned in SP 800-66 Revision 1 [4], "It represents an information security life cycle that facilitates continuous monitoring and improvement in the security state of the information systems within the organization."

The RMF includes the following six steps:

- Step 1 CATEGORIZE Information Systems per Federal Information Processing Standards (FIPS) 199/NIST SP 800-60. As described by SP 800-66 Revision 1 [4], "the first and arguably the most important step in the RMF, employs FIPS 199 and NIST SP 800-60 to determine the criticality and sensitivity of the information system and the information being processed, stored, and transmitted by the system."
- Step 2 SELECT Security Controls FIPS 200/SP 800-53. As mentioned by SP 800-66 Revision 1 [4], "the second step in the RMF, employs FIPS 200 and NIST SP 800-53 to identify and specify appropriate security controls for the information system. "
- Step 3 IMPLEMENT Security Controls SP 800-70. As noted by SP 800-66 Revision 1 [4], "the third step in the RMF, employs enterprise architectures,

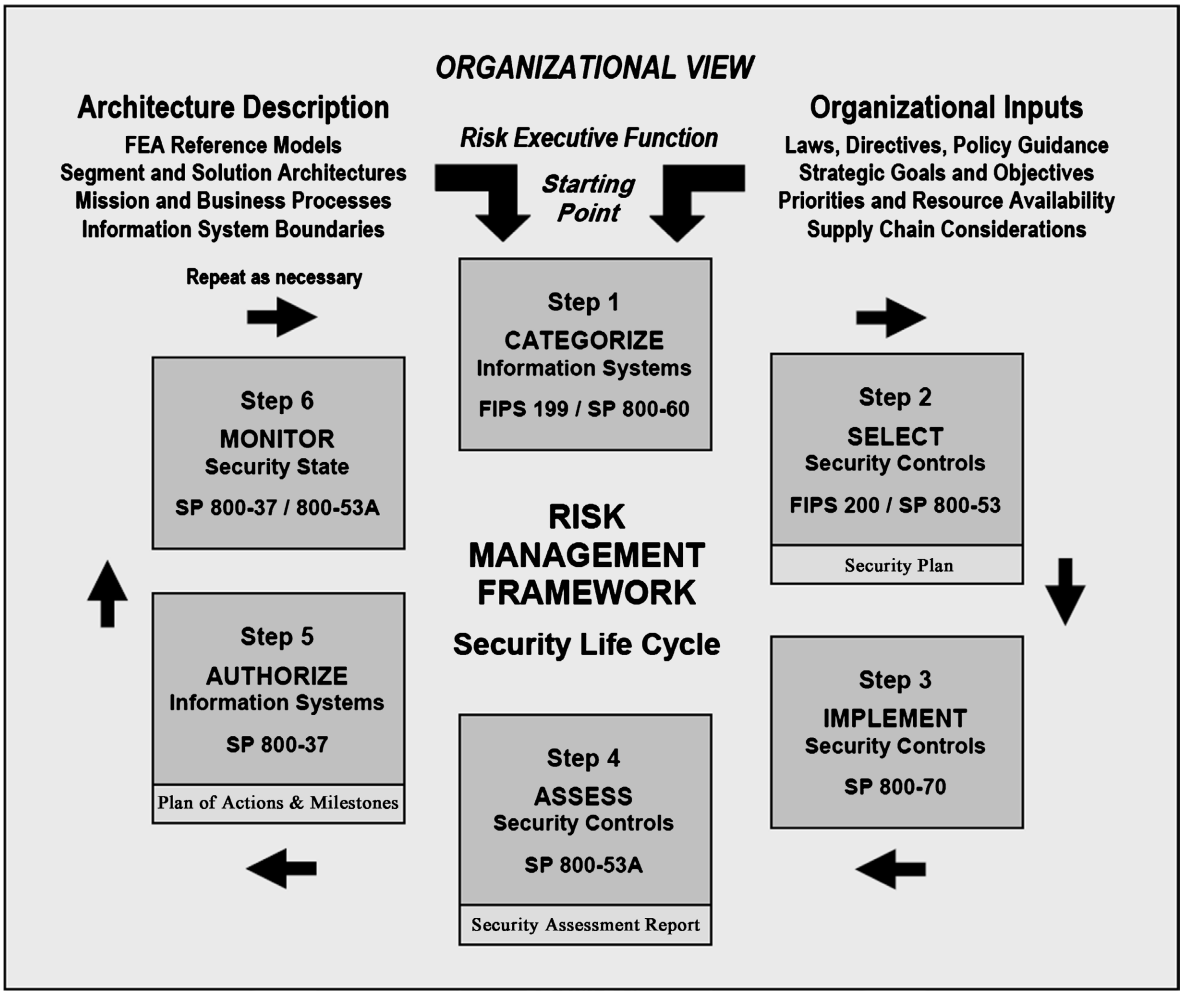

Figure 1. NIST risk management framework.

the System Development Lifecycle (SDLC), and various NIST publications to guide the implementation of security controls in organizational information systems."

- Step 4 ASSESS Security Controls SP 800-37. As documented by SP 800-66 Revision 1 [4], "the fourth step in the RMF, employs NIST SP 800-53A to evaluate the information system security controls for effectiveness using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security objectives and requirements for the system."
- Step 5 AUTHORIZE Information Systems SP 800-53A. As written by SP 800-66 Revision 1 [4], "Authorize information system operation (with implemented security controls) based upon a determination of the risk to organizational operations, organizational assets, individuals, and other organizations, and an explicit decision to accept this risk."
- Step 6 MONITOR Security State SP 800-37/800-53A. As outlined by SP 800-66 Revision 1[4], "Threats and vulnerabilities to an operating environment, as well as safeguards designed to combat them, can change frequently. The assessment and evaluation of security controls on a continuous basis provides oversight and monitoring of the security controls to ensure that they continue to operate effectively and as intended."

The variety of standards involved in the RMF (e.g., FIPS 199 and NIST SP 800-60) is also used by industries other than healthcare. However, the SP 800-66 Revision 1 was withdrawn in February 2024 and superseded by SP 800-66 Revision 2. As indicated in the SP 800-66 Revision 2, "this publication provides practical guidance and resources that can be used by regulated entities of all sizes to protect ePHI and better understand the security concepts discussed in the HIPAA Security Rule" [6]. Since it is in draft form and not ready for use in production, papers that reference Revision 2 and not Revision 1 will be excluded.

As defined above, the research problem concerns the incidence rate of US healthcare breaches. However, in reviewing the former studies on relevant problems, A study conducted in 2020 [7] addressed the role of awareness of Health Information Technologies (HIT) standards for industry policy and decision-makers. Their study targeted the factors influencing the adoption of HIT standards in healthcare organizations. They found that, among other things, awareness of the standard and reporting on adoption can raise awareness and promote further adoption."

Moreover, Rogers [8] posited that diffusion of innovation was fundamentally based on awareness of innovation, which explores how new ideas spread within societies. Rogers identifies different types of factors and adopters influencing adoption rates. Additionally, Hasani, O'Reilly, Dehghantanha, Rezania, and Levallet studied the problem concerning the role of cybersecurity adoption in enhancing organizational performance. Their finding had a positive impact on the relationship between the adoption of cybersecurity technologies and organiza-

tional performance [9].

From an awareness standpoint, this study aims to examine and assess the inclusion of SP 800-66 Revision 1 in the US healthcare academic literature. Potentially, we can understand the current impact of the literature on the awareness of US healthcare security practitioners. Understanding the literature can possibly help to predict whether additional academic papers pertaining to SP 800-66 Revision 2 in the US healthcare literature are needed.

2. Methodology

A systematic review research method was used in this study. According to Jalonen [10], "A systematic literature review is a trustworthy, rigorous, and auditable methodology for evaluating and interpreting previous research relevant to a particular phenomenon of interest." This study aims to include eligible academic papers based on advanced search criteria, and the data is collected from the existing literature. Therefore, this study employed a systematic literature review method. One of the significant advantages of this method is its ability to reduce bias in addressing the research question [11]. This section includes sub-sections that explain the eligibility criteria, research question, data collection, and inclusion and exclusion of the studies.

2.1. Definition of the Eligibility Criteria

Since the research problem is targeting the breaches in the US healthcare industry, the reviewer set the eligibility requirements for the study to select and review all papers addressing the healthcare domain and settings in the US, except those papers that are non-related to the Health Information Systems (HIS), such as disease academic papers. Typical examples of the HIS are Electronic Medical Records (EMR) [12], Personal Health Records (PHR) [13], and Electronic Health Records (EHR) [14].

2.2. Research Question

As mentioned in the introduction section, the SP 800-66 Revision 1 standard clearly targets the readers' healthcare security awareness. Our research question is formed based on readers' awareness. The readers could be any type of people, including healthcare security practitioners. However, Schlögl and Stock [15] found a low level of information exchange between practitioners and academic journals.

In this study, the researcher wondered how the National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1 was utilized in academic studies within the existing literature, specifically within the US healthcare industry.

2.3. Data Collection Sources & Strategy

This study relies on secondary data sources from the existing literature. The

search was for the keyword "SP 800-66" in the Google Scholar database engine conducted in June 2023. The date range of the search was set from 2008 to 2024. The reason behind setting 2024 as an end date is to show all of the existing papers. In addition, the author attempts to search in the Google Trends search engine, but it shows no results for the period from January 1, 2008, to January 1, 2023, when searching for the SP 800-66 keyword. However, the data collected for this study is sourced from the Google Scholar database engine only. The data collection processes for the study have an inclusion perspective and an exclusion perspective.

2.4. Inclusion & Exclusion of the Studies

The exclusion perspective rejects papers with SP 800-66 Revision 2, non-English academic papers generally, papers with no publishing dates, and non-academic papers such as books and class research projects. In addition, the exclusion is also applied to papers that mention SP 800-66 in the reference section and are not cited in the paper's content.

The inclusion perspective includes the academic papers that are:

- Full research paper, for example, not an abstract, not a poster, not a presentation, not a student thesis, not a book, not a book's chapter, and not surveys.
- The research paper includes the keyword "SP 800-66" and its relevant citation in the content of the paper.
- The research paper should clearly demonstrate relevance to health information systems listed in the Google Scholar database within the specified date range.

Figure 2 illustrates a systematic review flow diagram, which contains the identification phase, inclusion phase, and exclusion phase; it shows the structure and the total number of papers found in the systematic review study. As shown, the inclusion phase represented the selected eligible studies, while the exclusion phase represented the non-eligible studies.

A total of 540 studies were identified in the preliminary search in the Google Scholar Database. The researcher excluded 529 studies from this review because

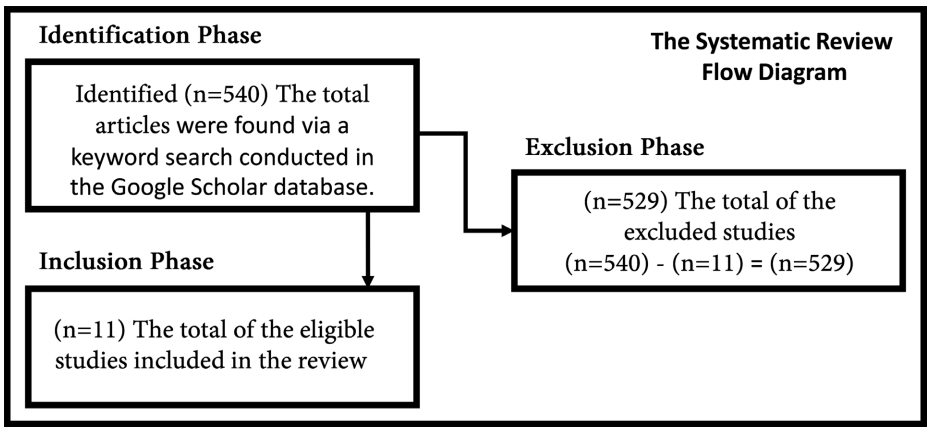

Figure 2. The flow diagram of the systematic review.

they did not meet the study's eligibility criteria. That reduced the identified papers from 540 studies to 11 eligible studies, which represent the sample data, and they are listed in Table 2. Details of the excluded paper triggers are in the discussion section below.

3. Results

Eleven eligible papers were reviewed, and their data were synthesized and analyzed in the study. Table 2 displays the overview of these articles; they are listed chronologically by publishing year.

From the perspective of reflexivity in evaluating intercoder reliability, O'Connor and Joffe [16] discussed that the same researcher returns to the data at another time. However, the reviewer reviewed these eligible studies three times over three different periods. The researcher added the "what specific topics are covered?" column in Table 2 for reliability, the researcher documented the

Table 2. The observation of the eligible papers.

Authors' citation	What specific topics are covered?	How was SP 800-66 Revision 1 used?	Publishing Year
(Gikas, 2010) [17]	Regulatory Compliance Requirements	It was used as an example of one of the sources for implementing the requirements of the HIPAA Security Rule.	2010
(Pagano & Peterson, 2010) [18]	Regulatory Compliance Requirements	It was used as a reference for access controls on electronic devices	2010
(Ghafarian & Smith, 2011) [19]	Risk Assessment	It was used as an example of one of the risk assessment methodologies used by United States healthcare	2011
(Avancha *et al.*, 2012) [20]	Confidentiality, Integrity, Availability (CIA).	It was used as a source to address privacy. Particularly in healthcare mobile technology	2012
(Rahman & Kreider, 2012) [21]	Electronic Medical Record (EMR)	It was used as a source to explain confidentiality in healthcare organizations	2012
(Alaqili, 2013) [22]	HIPAA Security Rule.	It was used as a source in developing questionnaires for risk assessment reports in the healthcare domain	2013
(Meyer *et al.*, 2016) [23]	Security Controls	It was used as a Security and privacy requirement for systems, including healthcare organizations	2016
(Aranha *et al.*, 2019) [24]	Industrial Internet of Things (IIoT) and Interoperability	It was used as a security standard to describe the security requirements for all types of healthcare environments including medical devices.	2019
(Valluripally *et al.*, 2019) [25]	Regulatory Compliance Requirements	It was used as a security standard to configure cloud-based system healthcare domain involving Big Data	2019
(Jabangwe & Nguyen-Duc, 2020) [26]	IoT healthcare software	It was used as an example of the security standard in the United States, particularly from the regulation of the healthcare domain	2020
(Wilkinson *et al.*, 2021) [27]	HIPAA Security Rule Requirements for the Electronic Medical Record (EMR)	It was used as a reference for the Health Insurance Portability and Accountability Act (HIPAA) because EMRs contain patient event logging data, and Protected Health Information (PHI), which are originally mandated by the Security Rule in HIPAA	2021

inclusion reasons of eligible articles to help the readers understand and evaluate the reliability of this review.

4. Discussions

4.1. From an Exclusion Paper Perspective

This study found that 529 papers were non-eligible for review. As previously stated, the author's criteria required that the non-United States papers be excluded from the study. In accordance with what was observed, many non-United States relevant healthcare papers mentioned the keyword SP 800-66, such as Australia [28], Canada [29], Italy [30], Korea [31] [32], Malaysia [33], and Pakistan [34].

Nevertheless, it was difficult to determine the relevance of certain papers to the US healthcare industry, especially for healthcare technology papers, such as health Internet of Things (IoT) devices. Health IoT devices are growing in usage everywhere nowadays, not only in the US, such as the implantable pacemakers. There were challenges due to the absence of country mentions within these papers, making it unclear whether they pertained to the US or not. For example, Ngamboé *et al.* [35] primarily focused on the security scope of telemetry-enabled cardiac implantable electronic devices (CIED).

In addition, the SP 800-66 was found in a security education paper [36]. Spears [36] developed a course syllabus targeting IT students interested in health care. The course aims to provide students with real-world service-learning in risk assessment, and it includes SP 800-66 Revision 1 as free reading material, as one of many industry security standards in general.

4.2. From an Inclusion Paper Perspective

Eleven papers were eligible for review; the papers explored various technological domains in healthcare, including topics in Big Data analytics [25], Electronic Medical Record (EMR) [27], Risk Assessment [19], Mobile Technology [20], Industrial Internet of Things (IIoT) and Interoperability [24], Internet of Things (IoT) and Software [26].

Overall, the citations of NIST SP 800-66 Revision 1 address several quotations in eligible papers, the majority of them are about:

- Implementing the Requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.
- Regulatory Compliance Requirements.
- Security Controls.
- Confidentiality, Integrity, Availability (CIA).
- Risk Assessment.

Figure 3 shows the publishing years of these papers were as follows: 2010 (two papers), 2011 (one paper), 2012 (two papers), 2013 (one paper), 2016 (one paper), 2019 (two papers), 2020 (one paper), and 2021 (one paper). The study did not find any eligible published papers in these years: 2008-09, 2014-15, 2017-18,

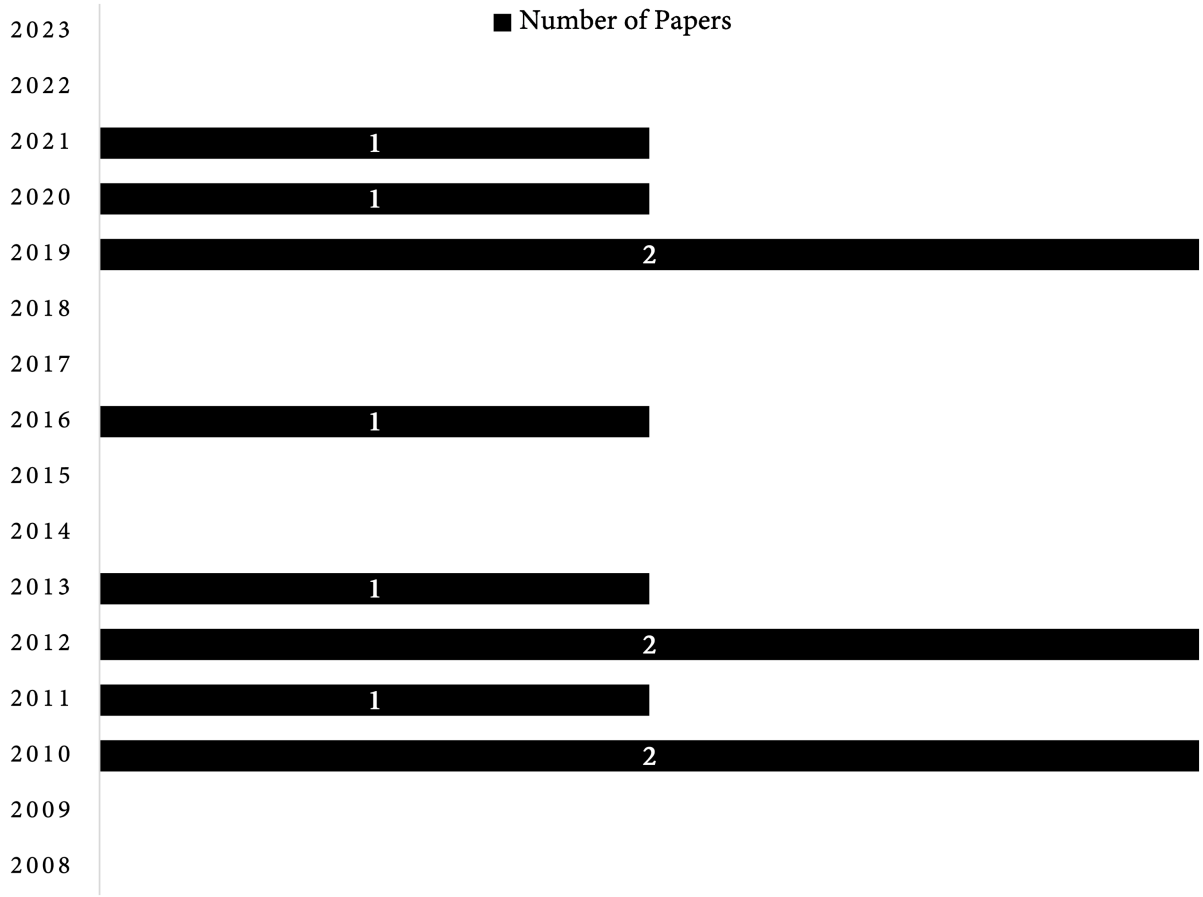

Figure 3. Number of eligible papers by publishing year.

2022, and 2023.

Lebek *et al.* [37] conducted a study on employees' Information Security (IS) awareness and behavior, they stated "in literature, there is consent (sic; consensus) that employees are the weakest link" in information systems security; they concluded, "the literature review might also be useful for practitioners that need information about behavioral factors that are critical to the success of an organization's security awareness."

However, based on the findings in this study, the reviewer believes it is essential to get greater academic visibility for SP 800-66 Revision 2 via citations in US healthcare papers since SP 800-66 Revision 1 has been retired. This study suggests using the SP 800-66 Revision 2 more frequently in academic papers that target the US healthcare industry. In turn, it will help to achieve the original objectives of the SP 800-66 Revision 2 and minimize future data breaches.

To illustrate, IoT and Artificial Intelligence (AI) are currently among the trending areas in healthcare, and their integration and development are ongoing. Presently, these areas have many gaps in terms of security and privacy breaches. Therefore, addressing the SP 800-66 Revision 2 in the IoT and AI, specifically in the US healthcare paper, will increase awareness of the security requirements.

Additionally, the author observed that not all health IoT papers address the

country name or specify the US healthcare regulations. Therefore, the author suggests using the 800-66 Revision 2 in health IoT security papers to address health regulations for health IoT security and privacy papers. Moreover, the manuscript of the 800-66 Revision 2 indicated the scope of risk assessment "should include all removable media and portable computing devices (e.g., laptops, mobile devices) as well as the myriad of medical devices (e.g., Internet of Things [IoT] used in healthcare) that can store, process, or transmit ePHI" [6].

5. Limitations and Future Directions

This study selected the eligible papers based on the keyword search "SP 800-66" on the Google Search Engine. However, the following identified limitations may potentially impact the validity of this study:

- Involve other scholarly database engines in keyword searching, for example, conducting keyword searches within and with other than the Scientific Research Publishing Journal.

6. Conclusions

With healthcare data breaches continuing to occur in the US, it is important to investigate how the NIST SP 800-66 Revision 1 is expanded in academic papers targeting US healthcare. The NIST SP 800-66 Revision 1 was written in 2008, mainly to help reduce incidents in the US healthcare industry. However, this study looked for SP 800-66 Revision 1 in the literature; a keyword search was conducted within the Google Scholar search engine, with the specified data range spanning from 2008 to 2024.

This review shows that the SP 800-66 Revision 1 manuscript was used in the literature of other countries and for different industries. Only 11 papers targeted US healthcare in the following areas: Big Data analytics, Electronic Medical Record (EMR), Risk Assessment, Mobile Technology, Industrial Internet of Things (IIoT), Interoperability, Internet of Things (IoT), and Software.

The study concluded that more studies are needed to raise awareness of SP 800-66 Revision 2, which will help reduce the potential for future healthcare data breaches in the United States. Moreover, this study underscores the need for an increased volume of academic papers pertaining to NIST SP 800-66 Revision 2 in US healthcare and broadening their scope to encompass other US healthcare technology applications such as the Internet of Things (IoT) and Artificial Intelligence (AI).

Acknowledgements

The researcher expresses gratitude to all peer reviewers for their comments and feedback.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Ignatovski, M. (2022) Healthcare Breaches during COVID-19: The Effect of the Healthcare Entity Type on the Number of Impacted Individuals. *Perspectives in Health Information Management*, **19**, 1c.

[2] Neprash, H.T., McGlave, C.C., Cross, D.A., Virnig, B.A., Puskarich, M.A., Huling, J.D., Rozenshtein, A.Z. and Nikpay, S.S. (2022) Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, **3**, e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

[3] Dolezel, D. and McLeod, A. (2019) Cyber-Analytics: Identifying Discriminants of Data Breaches. *Perspectives in Health Information Management*, **16**, 1a.

[4] Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, L., Dancy, C. and Steinberg, D. (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg. https://Tsapps.Nist.Gov/Publication/Get_Pdf.Cfm?Pub_Id=890098

[5] Department of Health and Human Services (2017) Covered Entities and Business Associates. Department of Health and Human Services, Content Created by Office for Civil Rights (OCR).

[6] Marron, J. (2024) Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. https://doi.org/10.6028/NIST.SP.800-66r2

[7] Han, L., *et al.* (2020) Factors Influencing the Adoption of Health Information Standards in Health Care Organizations: A Systematic Review Based on Best Fit Framework Synthesis. *JMIR Medical Informatics*, **8**, e17334. https://doi.org/10.2196/17334

[8] Rogers, E.M. (1995) Diffusion of Innovations: Modifications of a Model for Telecommunications. In: Stoetzer, M.W. and Mahler, A., Eds., *Die Diffusion von Innovationen in der Telekommunikation*, Springer, Berlin, 25-38. https://doi.org/10.1007/978-3-642-79868-9_2

[9] Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D. and Levallet, N. (2023) Evaluating the Adoption of Cybersecurity and Its Influence on Organizational Performance. *SN Business & Economics*, **3**, Article No. 97. https://doi.org/10.1007/s43546-023-00477-6

[10] Jalonen, H. (2012) The Uncertainty of Innovation: A Systematic Review of the Literature. *Journal of Management Research*, **4**, E12. https://doi.org/10.5296/jmr.v4i1.1039

[11] Turney, S. (2024) Systematic Review: Definition, Example, & Guide. Scribbr. https://www.scribbr.com/methodology/systematic-review/

[12] Ludwick, D.A. and Doucette, J. (2009) Adopting Electronic Medical Records in Primary Care: Lessons Learned from Health Information Systems Implementation Experience in Seven Countries. *International Journal of Medical Informatics*, **78**, 22-31. https://doi.org/10.1016/j.ijmedinf.2008.06.005

[13] Lafky, D.B., Tulu, B. and Horan, T.A. (2006) Information Systems and Health Care X: A User-Driven Approach to Personal Health Records. *Communications of the Association for Information Systems*, **17**, Article 46. https://doi.org/10.17705/1CAIS.01746

[14] Jardim, S.V. (2013) The Electronic Health Record and Its Contribution to Healthcare Information Systems Interoperability. *Procedia Technology*, **9**, 940-948. https://doi.org/10.1016/j.protcy.2013.12.105

[15] Schlögl, C. and Stock, W.G. (2008) Practitioners and Academics as Authors and Readers: The Case of LIS Journals. *Journal of Documentation*, **64**, 643-666. https://doi.org/10.1108/00220410810899691

[16] O'Connor, C. and Joffe, H. (2020) Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, **19**, 2. https://doi.org/10.1177/1609406919899220

[17] Gikas, C. (2010) A General Comparison of FISMA, HIPAA, ISO 27000 and PCIDSS Standards. *Information Security Journal*: *A Global Perspective*, **19**, 132-141. https://doi.org/10.1080/19393551003657019

[18] Pagano, M.W. and Peterson, Z.N. (2010) Design and Implementation of Views: Isolated Perspectives of a File System. https://jscholarship.library.jhu.edu/server/api/core/bitstreams/e3d79a3e-b346-4d6c-8b4a-a5e401db2776/content

[19] Ghafarian, A. and Smith, T. (2011) Information Security Risk Assessment Analysis. *SAM* 2011: *Proceedings of the* 2011 *International Conference on Security & Management*, Las Vegas NV, 18-21 July 2011, 1.

[20] Avancha, S., Baxi, A. and Kotz, D. (2012) Privacy in Mobile Technology for Personal Healthcare. *ACM Computing Surveys*, **45**, 1-54. https://doi.org/10.1145/2379776.2379779

[21] Rahman, M. and Kreider, C. (2012) Information Security Principles for Electronic Medical Record (EMR) Systems. https://aisel.aisnet.org/amcis2012/proceedings/ISHealthcare/9/

[22] Alaqili, M.Z. (2013) Road Map to HIPAA Security Rules Compliance: Risk Analysis at Orbit Clinics.

[23] Meyer, A., Green, L., Faulk, C., Galla, S. and Meyer, A.M. (2016) Framework for Deploying a Virtualized Computing Environment for Collaborative and Secure Data Analytics. *eGEMs* (*Generating Evidence & Methods to Improve Patient Outcomes*), **4**, Article 4. https://doi.org/10.13063/2327-9214.1224

[24] Aranha, H., Masi, M., Pavleska, T. and Sellitto, G.P. (2019) Securing Mobile E-Health Environments by Design: A Holistic Architectural Approach. 2019 *International Conference on Wireless and Mobile Computing*, *Networking and Communications* (*WiMob*), Barcelona, 21-23 October 2019, 1-6. https://doi.org/10.1109/WiMOB.2019.8923479

[25] Valluripally, S., Raju, M., Calyam, P., Chisholm, M., Sivarathri, S.S., Mosa, A. and Joshi, T. (2019) Community Cloud Architecture to Improve Use Accessibility with Security Compliance in Health Big Data Applications. *Proceedings of the* 20*th International Conference on Distributed Computing and Networking*, Bangalore, 4-7 January 2019, 377-380. https://doi.org/10.1145/3288599.3295594

[26] Jabangwe, R. and Nguyen-Duc, A. (2020) SIoT Framework: Towards an Approach for Early Identification of Security Requirements for Internet-of-Things Applications. *e-Informatica Software Engineering Journal*, **14**, 77-95. https://doi.org/10.37190/e-Inf200103

[27] Wilkinson, K., Seo, K., Pierce, R., Tonellato, P., Kim, J.H. and Myers, D. (2021) Electronic Medical Record Specialty Group Comparison by Multinomial Logistic Regression. 2021 *IEEE* 9*th International Conference on Healthcare Informatics* (*ICHI*), Victoria, 9-12 August 2021, 415-421. https://doi.org/10.1109/ICHI52183.2021.00067

[28] Liu, V., Caelli, W., Yang, Y. and May, L. (2011) A Test Vehicle for Compliance with Resilience Requirements in Index-Based E-Health Systems. *Pacific Asia Conference*

on Information Systems, *PACIS* 2011: *Quality Research in Pacific Asia*, Brisbane, 7-11 July 2011, 13.

[29] Patel, A. (2011) Baseline Security Controls for HIA-Compliant EMR Systems Using a Tailored NIST RMF Approach. https://doi.org/10.7939/r3-zas1-ej88

[30] Carello, M.P., Spaccamela, A.M., Querzoni, L. and Angelini, M. (2023) A Systematization of Cybersecurity Regulations, Standards and Guidelines for the Healthcare Sector. arXiv: 2304.14955.

[31] Choi, A., Chung, K., Chung, S.P., Lee, K., Hyun, H. and Kim, J.H. (2022) Advantage of Vital Sign Monitoring Using a Wireless Wearable Device for Predicting Septic Shock in Febrile Patients in the Emergency Department: A Machine Learning-Based Analysis. *Sensors*, **22**, Article 7054. https://doi.org/10.3390/s22187054

[32] Kim, J. and Chang, H. (2020) A Study on Security Evaluation Model of Small and Medium-Size Healthcare Institutions. *ICIC Express Letters*, *Part B*: *Applications*, **11**, 705-712.

[33] Khan, S., Gani, A., Wahab, A.W.A., Bagiwa, M.A., Shiraz, M., Khan, S.U., Buyya, R. and Zomaya, A.Y. (2016) Cloud Log Forensics: Foundations, State of the Art, and Future Directions. *ACM Computing Surveys*, **49**, 1-42. https://doi.org/10.1145/2906149

[34] Gardazi, S.U. and Shahid, A.A. (2017) Compliance-Driven Architecture for Healthcare Industry. *International Journal of Advanced Computer Science and Applications*, **8**, 568-577. https://doi.org/10.14569/IJACSA.2017.080571

[35] Ngamboé, M., Berthier, P., Ammari, N., Dyrda, K. and Fernandez, J.M. (2021) Risk Assessment of Cyber-Attacks on Telemetry-Enabled Cardiac Implantable Electronic Devices (CIED). *International Journal of Information Security*, **20**, 621-645. https://doi.org/10.1007/s10207-020-00522-7

[36] Spears, J.L. (2018) Gaining Real-World Experience in Information Security: A Roadmap for a Service-Learning Course. *Journal of Information Systems Education*, **29**, 183-202.

[37] Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013) Employees' Information Security Awareness and Behavior: A Literature Review. 2013 46*th Hawaii International Conference on System Sciences*, Wailea, 7-10 January 2013, 2978-2987. https://doi.org/10.1109/HICSS.2013.192