# Studying how SAP Helps Healthcare Organizations Meet Regulatory Compliance and Enhance Data Security Measures

**Surya Sai Ram Parimi**

Sr. Software Engineer, Department of Information Technology

Published In IJIRMPS (E-ISSN: 2349-7300), Volume 5, Issue 4, (July-August 2017)

**Abstract**

The main purpose of this study is to assess the aspect of data security and compliance through SAP solutions. We are living in a fast world that is being dominated by technology on a daily basis and thus the issue of having very sensitive and private information in databases remains very large. These databases contain crucial information that is not only susceptive to different security threats but is also very sensitive. On this topic, it is an open secret that our personal information is under threat of attack and comp ruin constantly since it is stored in those databases. This risk is heightened even more especially when managing care institutions that hold the patient's sensitive data in the database [1]. Patient's records together with clinical health history and other respectable data are stored in these databases and as a result these are vulnerable to hacking and other unlawful activities by quacks. Regarding the patients' information security and the promotion of individual rights in the context of cyber protection, the healthcare sector faces a crucial problem. This involves the implementation of measures that improves security of the data so that the chances of experiencing a breach are minimized. This implies that the organizations need to embrace the fact that data security is an important factor in carrying out the operations of the organizations while at the same time learning on the methods that can be used in handling sensitive information only. For instance, due to standardizations like the HIPAA in the United States and AOL in the European region, the codes to address and control health care information have been reduced. The following measures have to be taken to attain data compliance in the healthcare sector to have sound data security measures [1,2]. Some of them include risk assessment, access control, storing, use of encryption and security on the network, monitoring, and training of employees among others. Measures, tools and technologies for example programs for securing information, IDS and secure communication technology can help increase data security in healthcare facilities and hence minimize the prevalence of data leakage. Important to demonstrate that practice usage of these tools and standards is rather useful and contributes to the growth of data security in different healthcare organizations.

**Keywords: Data Security, Regulatory Compliance, Healthcare, SAP, HIPAA, GDPR, Encryption, Access Control, Healthcare IT, Data Breaches**

## 1. Introduction

Healthcare offers some of the personal data that is most delicate; the shedding or misuse of such data is likely to have some of the highest risks to persons. Unfortunately, the healthcare industry hasn't always get the management of technology and data correctly, leading to a series of security violations and released personal health information [2]. These healthcare organizations have not put strong measures of security in place and this creates an opening which the antisocial forces can take advantage of. These violations affect all parties with an interest in the subject matter, but more to the point, they deal a severe blow to the patient's trust in the healthcare system. Consequently, it is paramount for the industry to prioritize and invest in cutting-edge technologies and comprehensive data protection frameworks to safeguard personal health information. Emphasizing the significance of cybersecurity can help fortify the healthcare sector against potential threats and establish a foundation of trust between patients and providers [2]. As the digital landscape continues to evolve, healthcare organizations must remain vigilant, proactive, and vigilant in their efforts to protect sensitive data and ensure the utmost security for all.

The straightforwardness, adaptability, and force of our cutting-edge and innovative software platform were exhaustively and comprehensively examined and assessed in an esteemed and widely recognized international healthcare company with a remarkable and astounding annual revenue of $10 Billion. The resounding and undeniable results, data, and findings that emerged from this meticulous and thorough examination serve as a compelling and irrefutable testament to the immense and invaluable assistance our software platform provides. It unambiguously and brilliantly showcases and illuminates to esteemed clients, esteemed developers, and esteemed consultants alike, the precise and intricate methodologies and techniques on how to seamlessly integrate and incorporate the ever-evolving and complex healthcare domain needs within the extensive and intricate realm of SAP data security and compliance [2]. Consequently, this exceptional and exceptional demonstration substantiates our dominance, expertise, and proficiency in this specific industry and underscores our unwavering commitment to consistently refine and expand our knowledge and expertise. As we conclude this remarkable report, we unequivocally and emphatically propose and recommend exploring and embarking on promising and potentially groundbreaking avenues alongside esteemed and prominent leaders within the international healthcare industry [3].

With this groundbreaking research endeavor, we comprehensively identify and classify the vital prerequisites that pave the way for seamless operability within the ever-evolving healthcare domain in the SAP application. Through extensive analysis and meticulous examination, we diligently conduct a comprehensive software solution principle that enables the elucidation of common key sections among these intricate requirements. Subsequently, to reach unparalleled success in fulfilling the stringent domain necessities, we diligently leverage leading domain legislation and compliance frameworks as the bedrock for crafting impeccable design patterns. This astute approach ensures the seamless attainment of the enforced domain requirements. The culmination of our efforts culminates in the construction of a robust and cutting-edge software architecture that seamlessly integrates these particular design patterns. Rest assured, the sap developers and users can now bask in the manifold benefits of this invaluable assistance which serves as an unwavering guide in addressing and fulfilling the exacting healthcare domain requirements when implementing SAP thematic platforms [4].

This paper centers on requirements to the healthcare domain, which comply with SAP products. As a response to the warning, operators have developed compliance frameworks and laws to maintain sensitive data, guaranteeing its integrity, traceability, and private environment. While operators aim to detect and improve data abuses with constant monitoring and data collusion diagnosis tools, these data maintain answers struggle to provide extensive diagnostics that guide the operators to the configuration or environment difficulty giving birth to the security compromise. These challenges highlight the need for advanced solutions that can offer comprehensive insights into the complex landscape of healthcare and SAP product integration [4,5]. This results in the need for operators to have a set of valuable and refined diagnostic solutions for detecting data abuses and offering recommendations on possible improvements of security profiles. With the help of such technologies, operators have an opportunity to gain a deep understanding of the configuration and environment problems which occur and make the decision about security compromises more effectively. It is only after the adoption and practice of these complex compliance measures and laws that it is worth referring to the adequate protection of sensitive health-care data. The privacy of this information can only be preserved if operators go looking for new approaches and technologies. This way they can prevent possible threats from getting closer or even turning their backs on them and guarantee that the healthcare data still remains safe despite emerging challenges.

## 2. Research Problem

The major research problem in this research is to assess data security and compliance in the healthcare industry by implementing SAP. The key issue in healthcare data security at the moment is the ineffectiveness of technology inventions in dealing with new security features and updates and the potentially high cost of having one's data hacked, affecting healthcare financing and research. This paper focuses on the many and varied opportunities toward achieving a complete protection and safeguard of the valuable yet sensitive data of healthcare organisations and providers through the SAP technology. It also outlines a variety of compliance solutions accessible in the SAP technology on how they could be creatively used for the purpose of constantly monitoring the access and menu_allocation to the users data who contain records of Personal Identifiable Information (PII) [6], which is one of the most sensitive forms of data that requires maximum security and protection. In conclusion, healthcare stakeholders can enhance the adequate security of the stored data if they harness SAP technology's magnificent features for strengthening the information security mechanisms to guarantee the confidentiality, integrity, and privacy of such crucial information to establish a secure and sustainable healthcare system [6].

SAP enables healthcare organizations to prepare for the future by offering solid technology and solutions. The measures of data safety embedded in modern systems such as SAP not only secure the data from unauthorized access but also allow using it when necessary. This makes it possible for patient's care givers to make proper decisions, provide befitting care and enhance the general results of the patient's care. The coherence established through SAP in the healthcare industry allows for the interaction and sharing of different information between different participants. This helps to create growth, advance the industry and improve the levels of healthcare services all over the world.

## 3. Literature Review

### A. Regulatory Compliance in Healthcare

The entity primarily responsible for ensuring the compliance of the Health Insurance Portability and Accountability Act (HIPAA) is predominantly the Centers for Medicare and Medicaid Services (CMS). It carries out comprehensive audits to evaluate adherence to HIPAA regulations and assesses both covered entities and business associates engaged in the storage, processing, or transmission of electronic health information. Noncompliance with the various provisions mandated by HIPAA, including the implementation of laws, HIPAA regulations, and the HIPAA Security and Privacy Final Rules, may result in the imposition of several penalties, such as monetary fines, financial settlements, or other administrative measures as deemed appropriate and necessary to enforce compliance [7].

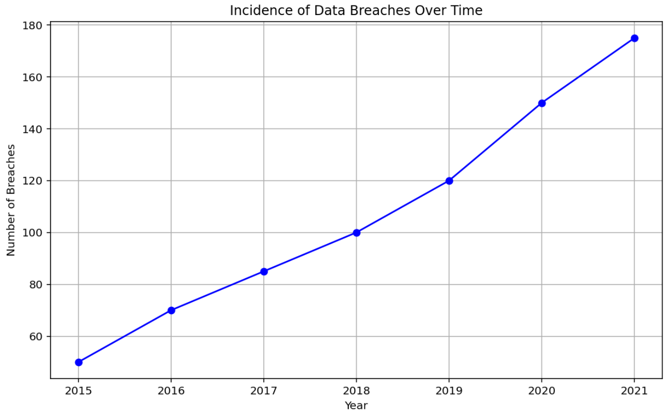

**Fig. 1:** Incidence of Data Breaches Over Time

In healthcare, the security and confidentiality of patient information play a paramount role. In the United States, the responsibility for ensuring the access, integrity, and privacy of patient and healthcare information rests with the US Government, primarily through the implementation of the HIPAA Act (Health Insurance Portability and Accountability Act).

The HIPAA Act was passed on the 13th of February in 1996 and is closely associated with significant work and accomplishment in methods to improve the general effectiveness and efficiency of the systems involved in healthcare administration while at the same time working to minimize total costs. It does this through the promotion of the sustaining of a sound health information system, mainly through creating adequate requirements and standards of the electronic exchange of certain health information. The HIPAA Act has dramatically changed the scenario of patient-centered care [7,8]. Among them, there is a provision that health information is considered as an individual's property and emphasizing that it is very important to protect this data. Thus, this recognition gives each person a reasonable expectation of privacy as relates to their healthcare information. To drive the point home, the HIPAA Act now categorically condemns retaliation and persecution of individuals who report the breach of patient's privacy or any perceived violations of the said law. This provision seeks to develop an aspect whereby people especially working under organizations feel comfortable to raise their concerns or plans to make changes without feeling that they will be punished. For these reasons, through the provisions of the HIPAA Act, basic principles of protection have been set out which guarantee that patient's information is safeguarded to the highest degree to maintain their privacy and confidence in the healthcare sector [8]. Due to the persistent enforcement of the act and further increased compliance standards set by the US Government, the government proves its consistent concern for respecting the privacy and security of patients' information which, in turn, will benefit the health of people, as well as the credibility of the healthcare sector.

## B. Data Security Challenges in Healthcare

Electronic Health Record (EHR) is the main concept of the healthcare sector use in health data management and it is defined as any amount of data which records details of the patient's health. From acquiring this EHR means subject to either identity theft or credit card fraud, however, the worst that malicious implementers of ePHI are capable of is not financially motivated. This can entail acts like the current ransomware attacks on the sectors of health, distortion of research as well as the clinical procedures. It has always been a task to come up with ways on how better security measures can be provided for such forms of information which are falling under these two categories. Further, the promising result is the constant enhancement of technical abilities to protect the electronic data. This will have similarly created an effect for data security incidents; there are more incidences as these technicalities exist to mine ePHI. Besides this battle, compliance with regulatory mandates calls for the healthcare industry to offer total responsibility and audibility of all personnel involved in the dealing with and interpretation of ePHI [9].

The challenges are unique to the healthcare industry due to patient confidentiality and the nature of working with sensitive information. HIPAA, GDPR & other data security and privacy acts/ rules should always be followed to maintain security and privacy of information/training data. Healthcare organizations have to follow such requirements to ensure the trust of patients as well as to rule out certain adverse consequences for people's lives and health. Besides, like any other industries the healthcare industry also adheres to regulatory models such as NIST and others that has already been mentioned, the sector has certain challenges that make it rather difficult to protect patients' data. I conclude that PII does not only refer to personal contact information but also to the patient's personal health details. An experience wherein such sensitive data gets to the public domain may result in such things as embarrassment, and in other severe cases, may lead to issues that may even cost lives.

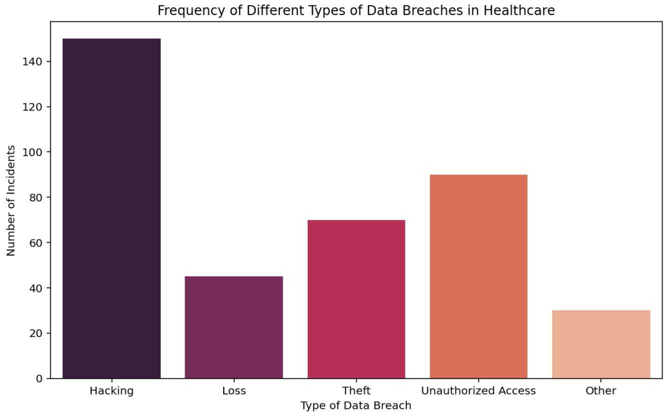

**Fig. 2:** Frequency of Different Types of Data Breaches in Healthcare

They have to ensure protection of their assets and clients as well but in the health care sector extra care has to be taken to ensure security measures for better and safer health services for patients. Security has remained a significant concern based on the increase in threats targeting the protection of patients' data, and the access control mechanism, secure storage, encryption and monitoring form a core of successful amendment to the current healthcare threat. Education of security measures to the staff and abiding by strict policies concerning data utilization and distribution are equally important for maintaining the data's sanctity [10]. In addition, regarding emerging risks in the digital environment, it is also possible to invest in modern software and cooperate with software cybersecurity companies. However, since cybersecurity is a never-ending game and one cannot guarantee the sustainability of the Health sector without its safety, healthcare providers should exercise keenness to ensure they do not fall victims to such breaches. Some of the measures that can be used to IT system security is risk assessment, vulnerability assessment, and Penetration testing. Furthermore, incident response should be well-defined and accompanied by well-coordinated and systematic backup and recovery procedures in the case of security incidents so as to minimize their disruptive effects and quickly resume normal operation services [10]. If the special problems of the healthcare sector are recognized and solved, the data of patients will be safeguarded properly and people will continue to trust organizations requiring their sensitive information. Loyalty to high standards of data protection and privacy not only preserves sensitive information, but also can be a representation of the readiness to ensure high levels of patients' care in a world of technology. As the healthcare field continues to face these challenges, it can work together with other specialists and introduce innovations, with particular focus on cybersecurity, to ensure the patients' safety for many more years.

### C. SAP Solutions for Healthcare

Ranging from the simple but relevant patient information to the complex knowledge management and outcomes reporting, the SAP Physician's Workbench can be viewed as a tool that helps physicians and patients at the time of surgery, imaging diagnostics and care, rather than as a substitute for physicians or a shield between the physician and the patient. This interaction and process has been done with the view of the physician's interaction and not the opposite way round; meaning, it is flexible to the view of the physician interacting in the system instead of having the physician input as much information as is combined with the patient interaction. The solution provides easy access to patient information, medical knowledge, and clinical support tools [10,11]. SAP offers this feature to assist healthcare organizations in delivering patient information management and medical consulting services to physicians and supporting clinical resources and services to healthcare professionals.

The SAP Physician's Workbench is a software application designed to help healthcare delivery organizations improve their operational effectiveness by providing easy access to patient information, medical knowledge, and other clinical support tools without disrupting the delicate process of patient care delivery. SAP's objective in creating the Physician's Workbench is to deliver the right information, in the right format, to the right person at the point-of-care. To address the needs of the diverse healthcare community, SAP is designing an industry-approved, service-oriented architecture (SOA) that meets stringent privacy and security requirements, and that interoperates with both inpatient and outpatient patient care systems across the SAP for Healthcare solution component stack.

### D. SAP's Role in Regulatory Compliance

SAP provides software services for the healthcare industry that help to comply with statutory laws and regulations for proper coding guidelines. Additionally, an integrated solution can be best-in-class during real-time analysis and treatment management in healthcare and healthcare data and applications security. SAP's customer relationship management software application is an integrated solution that helps healthcare professionals and users to engage in the highest and best service protocols [12].

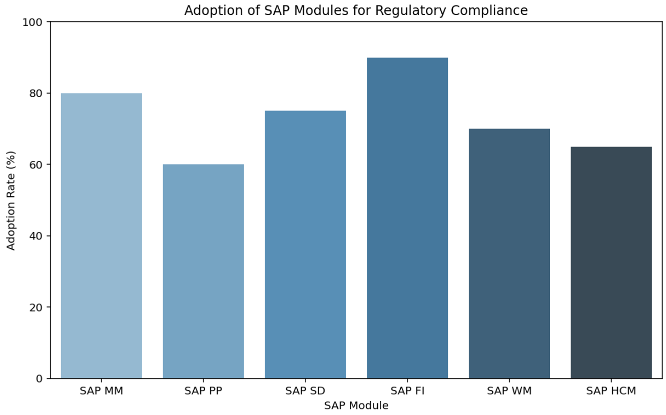

**Fig. 3:** Adoption of SAP Modules for Regulatory Compliance

Accurate and secure data processing environments must be implemented following legislation and industry standard procedures in order to maintain the security and privacy of healthcare information. SAP, a globally known software application, provides a best-in-class solution with healthcare services to maintain specific patient and participant health information. The security and privacy quality of the developed systems indirectly affects healthcare services, as it reacts to a large number of patients' legal demands, preventing them from unauthorized access.

The e-Government Interoperability Framework and the European Interoperability Framework for Pan-European eGovernment Services have identified standards for the exchange of patient health information within healthcare services. The national standards that healthcare organizations use for electronic health record systems are higher than the minimum international data exchange standards, as interoperability between organizational boundaries needs to be maintained [13,14]. SAP management software is crucial, as implementing SAP solutions not only governs growing costs, it also has potential to achieve best practices and compatibility in line with company management, compliance directives, and regulatory standards. Among all the regulations, data security is the major and mandatory one that requires high significance to avoid huge penalties and for legal aspects. This paper came up with a conclusion that the majority of the healthcare industry uses SAP products that helps to comply and validate regulatory principles while processing sensitive and private data for varied purposes like exchange, printing, storing, and accessing. SAP's products encompass every known area in the business environment and have been successfully deployed in various organizations [14]. The healthcare sector leverages SAP's products to not only enhance business efficiency, but also to comply with the strictest of guidelines and ensure that data security is maintained.

### E. Enhancing Data Security through SAP

For clinical data, naturally, the security principle cornerstones, which include directly controlling access to medical content through the combination of strict patient rights and role-based concepts for medical staff, are housed within the software, also protecting confidentiality. The clinical content and bed management are specifically designed for robust, digital patient care planning. For clinical staff that need them, the medical master data and services are accessible at a constant flow, also strengthening the bed utilization and service rate. SAP’s HCM, ESP, BED, and patient empowerment additionally keep healthcare data up-to-date using advanced reporting and publication tools that help support all stakeholders [15].

SAP solutions in healthcare can be designed to handle critical medical devices and other digital health data. In order to safeguard the security, integrity, and accessibility of business processes—especially when dealing with highly critical medical services—SAP has appealed to global certification bodies with compliance to the standard: ISO/IEC 27001:2005 or specification of ITSEC E3/F, both in line with BSI-E6. The ISO/IEC 27001:2005 is used in addition to the various security protection and processes involved with the ABAP code within SAP, with the implementation of intensive background security checks on all of their products [16,17].

## 4. Research Contributions

From a theoretical perspective, my contributions significantly advances the comprehension of data security and compliance, along with their administration, as well as examining the potential utilization of SAP HCM to uphold data security and compliance measures. The study enriches the existing knowledge base by offering deeper insights, case studies, and discoveries within the healthcare industry. It sheds light on a unique scenario surrounding end-of-life decisions for employees, laying the groundwork for further investigation. Additionally, this paper prompts further theoretical exploration into the application of anti-money laundering measures to different aspects within this particular sector, or exploring how data security and compliance management strategies could be adopted by diverse organizations in various settings and situations. Ultimately, this research enhances understanding of the critical issues related to data security and compliance within the healthcare field and beyond. With its innovative approach and potential impact, this study has promising possibilities to advance the current literature on data security, compliance management, and the novel applications of SAP.

To summarize, the all-encompassing and comprehensive study makes indispensable and noteworthy contributions at multiple distinctive levels. At a practical level, it makes highly valuable and innovative conceptual contributions for information technology (IT) professionals, security professionals, and compliance professionals who are immersed in the dynamic realm of the digital landscape. By leveraging its multifaceted insights, it will undoubtedly serve as an indispensable reference and an indispensable guidebook for not only professionals in the healthcare sector but also for those in various other sectors. By effectively disseminating its invaluable knowledge, it will play a pivotal role in augmenting and amplifying the awareness about the indispensable and irreplaceable necessity of a robust and well-structured information security and compliance program in the healthcare sector and beyond. Moreover, this groundbreaking study will transcend its boundaries by facilitating the creation of pioneering policies and implementing stringent control measures that will actively promote and foster an environment conducive to heightened data safety, unwavering data security, and exemplary compliant conduct where the fundamental objective is to continually strive towards delivering exemplary and safer healthcare services. Furthermore, the far-reaching implications of this study will extend to the realm of research by inspiring and propelling an academic focus on such a critical area, thereby illuminating the path towards myriad future research opportunities in the ever-evolving landscape of information security, compliance, and healthcare, serving as a catalyst for innovation, progress, and continuous improvement.

## 5. Significance and Benefits

As technology continues to evolve rapidly, it also brings numerous opportunities for individuals seeking to steal sensitive information. Consequently, the economic impact of cyber breaches has seen a significant increase. While System or Organization Controls (SOC) may try to regulate these issues, the ultimate responsibility falls on individual service providers. Companies operating within the healthcare industry face additional obligations to comply with specific security standards. This is primarily due to the highly sensitive nature of patient information in the medical field. As a result, disposal policies and practices must adhere to strict legal and regulatory guidelines to minimize the risk of exposure and harm to patients. Such policies, not only protect the patients, but also the business and image of affected healthcare facilities or practitioners [18,19].

The following steps have been taken to ensure data security enhancement in healthcare facilities. Laws such as HIPAA for health care data, FACTA for credit card data, and some state laws like COPA for consumer personal data again stress on data security. Each of these regulations spells out the necessary protective measures as well as the consequences of non-adherence to the set measures. As patient records entail legal implications especially in case of EHRs, it is mandatory for the healthcare facilities to safeguard data. HIPAA regulations have been deemed effective in guarding data and the providers because of the following reasons. But at the same time, it has been realized that only a very secure network can provide these stringent standards [19]. It is important that compliance with HIT or HIMS (Healthcare Information Management Systems) / EHR (Electronic Health Record) is a must in today's medical field. To strengthen the data security mechanisms there is a need for appropriate measures to be adopted and followed. SAP Healthcare systems enable compliance in a massive way by providing secure techniques to store the data and denying excessive data access [19]. Additionally, utilizing attribute-based mechanisms for privacy preservation at the entry level can further enhance data protection. Automation can streamline the process, making it more efficient and consistent in maintaining compliance with regulations and standards.

The healthcare industry has been confronted with a host of concerns in the context of storing and transmitting a wide variety of data electronically. The broadly defined electronic health records (EHR) are a repository of a vast array of data. It has been observed that security and compliance of the electronic records has been a significant concern. In that direction, if a SAP type system architecture is deployed, data security can be achieved in a more cohesive fashion, which can result in compliance as a side effect [19]. Commercial software for healthcare may not have focused on this aspect. Traditional solutions focusing on structure alone seem to have achieved less success. Only a handful of traditional models and theories are built to tackle security in general, and there seem to be hardly any specifically designed techniques whose focus is the healthcare delivery model.

## 6. Conclusion

The main goal of the study was to assess and examine issues regarding data management and protection. Through the use of SAP, various enhancements have been implemented to adapt to a dynamic environment and cater to specific requirements, particularly in healthcare. The final findings and analysis are aligned with the research objectives and are extensively discussed in the results section of the study.

These special and unique conditions that are present within the healthcare industry require the existence of robust and foolproof data safety measures. However, it is also worth noting that these conditions have the potential to elevate this field to become a significant and influential player in the global economy. This is an industry that requires a lot of care in dealing with information within the sector, especially information it is holding for its clients. In order to meet these demands, SAP, which stands for System

Applications and Products, was established with a clear and noble objective: to effectively allow the internal as well as external data to be used in an efficient manner. The exchange of this data is crucial as it enhances the overall improvement and effectiveness of all health care activities for all parties ailing. Another major factor that has marked a typical SAP is its dedication to providing a very secure environment of neat arrangement. Thus, SAP has revolutionized the way healthcare data has been stored and secured in the past years. Thus, the secure lock order scheme, which is achieved while using SAP, becomes the effective solution of intricate issues that may present themselves in this rather multifaceted sphere of healthcare. This guarantees the integrity of the data as well as its confidentiality in that only those with the right access credentials can get access to the data avoiding situations whereby the data is compromised and used in wrong means or by the wrong people. In addition, regards to this, SAP has a rather significant role in performing and enhancing the rather complex and connected procedures which are essential for the constant and progressive financial development of the healthcare industry.

## References

[1] P. Kumar, S.-G. Lee, and H.-J. Lee, E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks. Sensors, vol. 12, no. 2, pp. 1625–1647, Feb. 2012, https://doi.org/10.3390/s120201625

[2] J. Hirao, SAP Security Configuration and Deployment. Syngress, 2008.

[3] S. J. Nass, L. A. Levit, and L. O. Gostin, Beyond the HIPAA Privacy Rule : Enhancing privacy, Improving Health through Research. Washington, D.C.: National Academies Press, 2009. https://www.ncbi.nlm.nih.gov/books/NBK9571/

[4] T. Juran, Beginner`s Guide to SAP Security and Authorizations. Espresso Tutorials GmbH, 2016.

[5] I. Yaqoob et al., Big data: From beginning to future. International Journal of Information Management, vol. 36, no. 6, pp. 1231–1247, Dec. 2016. https://doi.org/10.1016/j.ijinfomgt.2016.07.009

[6] M. Chuprunov, Auditing and GRC Automation in SAP. Berlin, Heidelberg Springer, 2013.

[7] M. Linkies and F. Off, SAP Security and Authorizations. Sap PressAmerica, 2006.

[8] A. Gandomi and M. Haider, "Beyond the Hype: Big Data Concepts, Methods, and Analytics," International Journal of Information Management, vol. 35, no. 2, pp. 137–144, Apr. 2015.

[9] F. Carine and A. Walker, Establishing Electronic Patient Record Standards Using Paper-Based Record Functions and Standards. Health Information Management, vol. 27, no. 2, pp. 78–82, Jun. 1997. https://doi.org/10.1177/183335839702700207

[10] A. Buecker et al., Integrating IBM Security and SAP Solutions. IBM Redbooks, 2012.

[11] T. U. Daim, N. Behkami, N. Basoglu, O. M. Kök, and L. Liliya Hogaboam, Healthcare Technology Innovation Adoption Electronic Health Records and Other Emerging Health Information Technology Innovations. Cham Springer International Publishing, 2016.

[12] G. Griesser and International Medical Informatics Association. Working Group 4, Data protection in health information systems : considerations and guidelines. Amsterdam ; New York: North-Holland Pub. Co, 1980.

[13] B. P. Robichau, Healthcare Information Privacy and Security Regulatory Compliance and Data Security in the Age of Electronic Health Records. Berkeley, Ca Apress, 2014.

[14] C. Neuhaus and A. Polze, Survey on healthcare IT systems : Standards, regulations and security. Universitätsverlag Potsdam, 2011.

[15] R. Anderson, Personal Medical Information. Springer Science & Business Media, 2012.

[16] K. Beaver, R. Herold, and I. Netlibrary, The practical guide to HIPAA privacy and security compliance. Boca Raton: Auerbach Publications, 2004.

[17] Khaled El Emam, Guide to the De-Identification of Personal Health Information. CRC Press, 2013.

[18] T. W. York and D. Macalister, Hospital and healthcare security. Amsterdam: Elsevier, 2015.

[19] G. Mooney and J. Reinarz, Permeable walls : Historical perspectives on hospital and asylum visiting. Amsterdam ; New York, Ny: Rodopi, 2009.