Received: 17 June 2024 | Revised: 9 September 2024 | Accepted: 13 November 2024 | Published online: 19 November 2024

REVIEW

Journal of Data Science and Intelligent Systems
2024, Vol. 00(00) 1–14
DOI: 10.47852/bonviewJDSIS42023640

GDPR Compliance of Hospital Management Systems in the UAE

Inas Al Khatib[1],* , Norhan Ahmed[1] and Malick Ndyiaye[1]

[1]*Department of Industrial Engineering, American University of Sharjah, UAE*

Abstract: While the United Arab Emirates (UAE) is making strides in healthcare digitalization and adopting global best practices, the absence of a unified data protection framework equivalent to the GDPR poses significant challenges for hospital management systems (HMS) in the region. This gap creates uncertainties in compliance, especially regarding cross-border data transfers, third-party vendor management, and the protection of patients' privacy rights. The lack of clear regulations tailored to the UAE's unique healthcare landscape hinders the implementation of robust data protection measures, raising concerns about potential data breaches, legal liabilities, and the overall trustworthiness of healthcare institutions. Addressing these challenges is crucial for aligning the UAE's healthcare sector with international standards while ensuring the security and privacy of patient data in a rapidly evolving digital environment. The General Data Protection Regulation (GDPR) has significantly impacted HMS by setting strict data protection requirements. This study provides a systematic literature review of GDPR compliance in HMS, focusing on key challenges such as regulatory complexity, permission management, data subject rights, data breaches, third-party vendor management, and cross-border data transfers. Suggested mitigation measures include privacy by design, data protection impact assessments, improved consent management, robust breach detection, and efficient vendor management. Legislative reforms are needed to clarify GDPR's application to healthcare. The study also highlights increased investments in privacy technologies, improved patient trust, and the demand for advanced solutions. Future research should explore the effectiveness of these mitigations, GDPR's impact on patient satisfaction, ethical data processing, and standardized data protection frameworks in healthcare. Achieving GDPR compliance is crucial for protecting patient data, building trust, and ensuring secure and ethical use of healthcare information. This study aims to guide healthcare organizations, particularly hospitals, along with regulators and researchers, in navigating these challenges and implementing effective solutions.

Keywords: GDPR compliance, health data protection, hospital management systems, general data protection regulation

1. Introduction

The healthcare industry, in particular, collects, stores, and processes vast amounts of sensitive patient information, making the protection of personal data and privacy a top priority in the modern digital era [1]. While the United Arab Emirates (UAE) is making strides in healthcare digitalization and adopting global best practices, the absence of a unified data protection framework equivalent to the GDPR poses significant challenges for hospital management systems (HMS) in the region. This gap creates uncertainties in compliance, especially regarding cross-border data transfers, third-party vendor management, and the protection of patients' privacy rights. The lack of clear regulations tailored to the UAE's unique healthcare landscape hinders the implementation of robust data protection measures, raising concerns about potential data breaches, legal liabilities, and the overall trustworthiness of healthcare institutions. Addressing these challenges is crucial for aligning the UAE's healthcare sector with international standards while ensuring the security and privacy of patient data in a rapidly evolving digital environment.

This paper aims to explore the profound implications of the General Data Protection Regulation (GDPR) on HMS and the healthcare sector as a whole. The GDPR, which came into effect in May 2018, was introduced with the overarching objective of protecting individuals' privacy by setting new, high standards for data protection across the European Union (EU) [2].

The regulation grants individuals enhanced rights, such as the right to access their data, the right to have their data deleted, and the right to be informed about how their data is being processed. These provisions necessitate that organizations, including hospitals, adhere to stringent data protection requirements and maintain transparency in their data handling practices [2]. Due to the sensitive nature of healthcare data, the intricate data flows within healthcare organizations, and the involvement of multiple stakeholders in healthcare delivery, ensuring GDPR compliance poses distinct and significant challenges for HMS [3].

This paper contributes to the existing body of knowledge by examining the specific requirements that healthcare organizations must meet to align with GDPR standards. It also discusses the significant challenges these organizations face in ensuring compliance and explores potential strategies for overcoming these obstacles. Furthermore, the paper aims to provide actionable insights into the governance and accountability structures that healthcare organizations need to establish to effectively safeguard patient data in compliance with GDPR [4].

By investigating these aspects, the paper seeks to not only highlight the critical role of data protection in healthcare but also to offer practical recommendations for HMS to achieve and maintain GDPR compliance. The ultimate objective is to enhance the understanding of GDPR's impact on the healthcare industry

*Corresponding author: Inas Al Khatib, Department of Industrial Engineering, American University of Sharjah, UAE. Email: g00091914@aus.edu

and to support the development of robust data protection practices that prioritize patient privacy and security.

2. Research Methodology

2.1. Research approach

This study used a systematic literature review as its research approach. It entails locating and assessing previously published books, journal articles, and other resources concerning GDPR compliance in HMS. The systematic review methodology guarantees a thorough and objective evaluation of the subject, enabling the synthesis of current knowledge and the identification of research needs to answer the following research question: *How does the General Data Protection Regulation (GDPR) impact the compliance requirements and data protection practices of HMS in the healthcare industry?* This question focuses on the core objective of the paper: to investigate the effects of GDPR on HMS and how these systems can align with the regulation's stringent data protection standards.

2.2. Data sources

For this systematic review, the screening method we followed involved a multi-step process to ensure the selection of relevant and high-quality studies were included.

Database Search and Initial Screening: To compile pertinent data, a variety of data sources were used. The study conducted searches on Scopus database given its reliability and vast industry coverage using terms like "GDPR compliance", "hospital management systems", "health data protection", and "health record privacy". Additionally, respectable regulatory entities' websites were searched for formal rules and directives, such as the official GDPR website of the European Union and the websites of pertinent healthcare authorities. Publications from 2018 to 2024 that concentrated on GDPR compliance in the healthcare industry were included in the inclusion criteria for the literature search.

Bibliometric networks were generated using VOSviewer software, utilizing data from the Scopus database, to construct various bibliometric maps for this study. The results of an advanced search, comprising 1649 items, were exported to VOSViewer for network visualization, as depicted in Table 1, aiming to identify the leading countries in publications within this domain. Upon analysis of the 1649 search results, the top five countries that emerged were United Kingdom, United States, Italy, China, and India. These countries share common traits, such as a robust industrial landscape, significant investments in the healthcare sector, and prowess in technology advancement.

Initial Screening by Title and Abstract: titles and abstracts of the retrieved articles were screened to identify potentially relevant studies. Excluded studies that clearly do not meet the inclusion criteria.

Eligibility Criteria:

Inclusion Criteria:

- Studies that focus on GDPR compliance in healthcare or HMS.
- Articles discussing data protection practices in the context of healthcare published between 2018 and 2024 timeframe
- Studies published after the GDPR was implemented (post-May 2018).
- Peer-reviewed journal articles, conference papers, dissertations, book sections, or high-quality gray literature.

Table 1
Used search term combinations

Terms used	Results
health AND data AND protection AND GDPR AND compliance	144
health AND data AND protection AND hospital AND management AND systems	367
health AND data AND protection AND health AND record AND privacy	771
GDPR AND compliance AND hospital AND management AND systems	11
GDPR AND compliance AND health AND record AND privacy	25
hospital AND management AND systems AND health AND record AND privacy	331
TOTAL	1649

Exclusion Criteria:

- Studies or publications not related to GDPR or healthcare data protection.
- Non-English language studies, unless translation is available.
- Articles with insufficient data or lacking rigorous methodology.

Supplementary sources (gray literature) were essential due to the topic's industry relevance, so we expanded the search to reliable industry outlets. This yielded eight supplementary sources from outlets such as leading management consultancy firms such as PWC. Additionally, reliable industry guidelines and standards from the European Data Protection Supervisor, HIPPA, and UAE National Electronic Security Authority (NESA) were utilized.

Full-Text Review:

Full-Text Screening: Retrieved and reviewed the full text of articles that passed the initial screening to determine their relevance and quality. Used a standardized data extraction form to ensure consistency in assessing the studies.

Quality Assessment:

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses checklist was used to assess the methodological quality and risk of bias in the selected studies.

Peer Review

Double Screening: Had the second author act as a second reviewer independently screen a subset of the articles to validate the consistency of the inclusion/exclusion process. Furthermore, resolved any discrepancies through discussion or involving our third author as a third reviewer.

Bibliometric networks were generated using VOSviewer tool as demonstrated by Figures 1–3, to depict the connections between authors through their publications. This analysis identified the leading countries in GDPR compliance research, with India at the forefront, followed by USA and China.

Figure 1
VOS network visualization

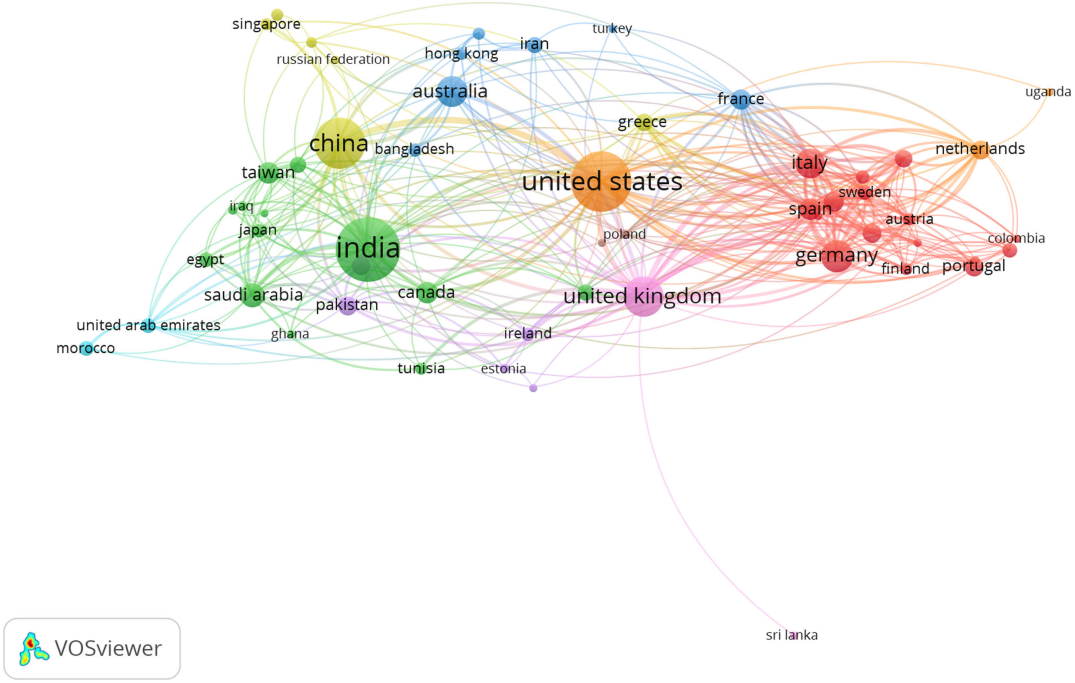

Figure 2
VOS overlay visualization

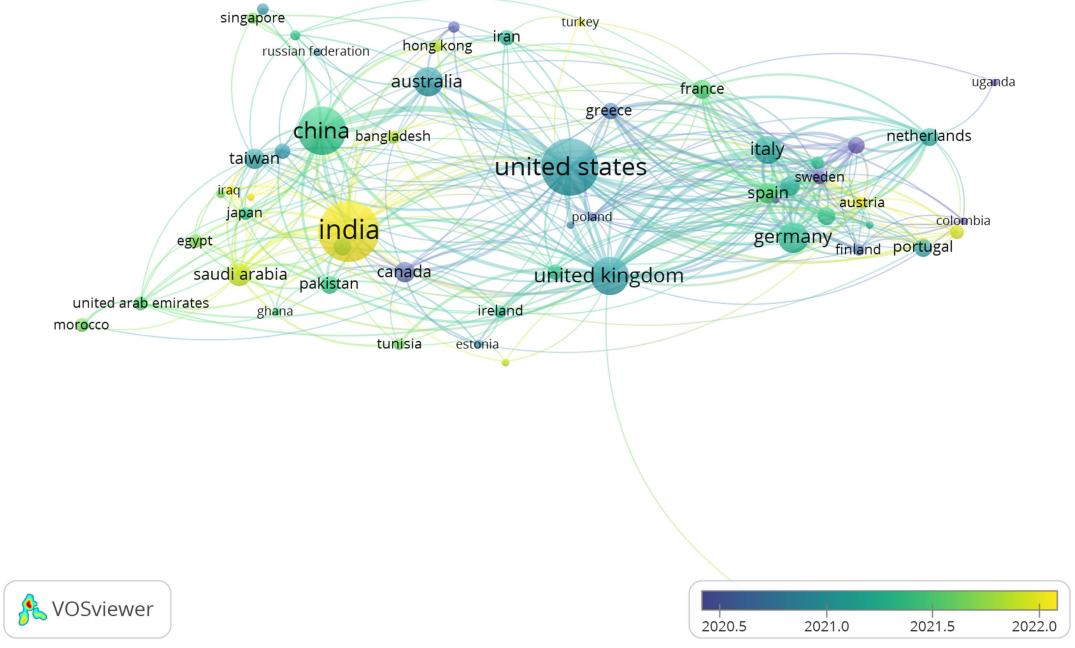

Figure 3
VOS density visualization

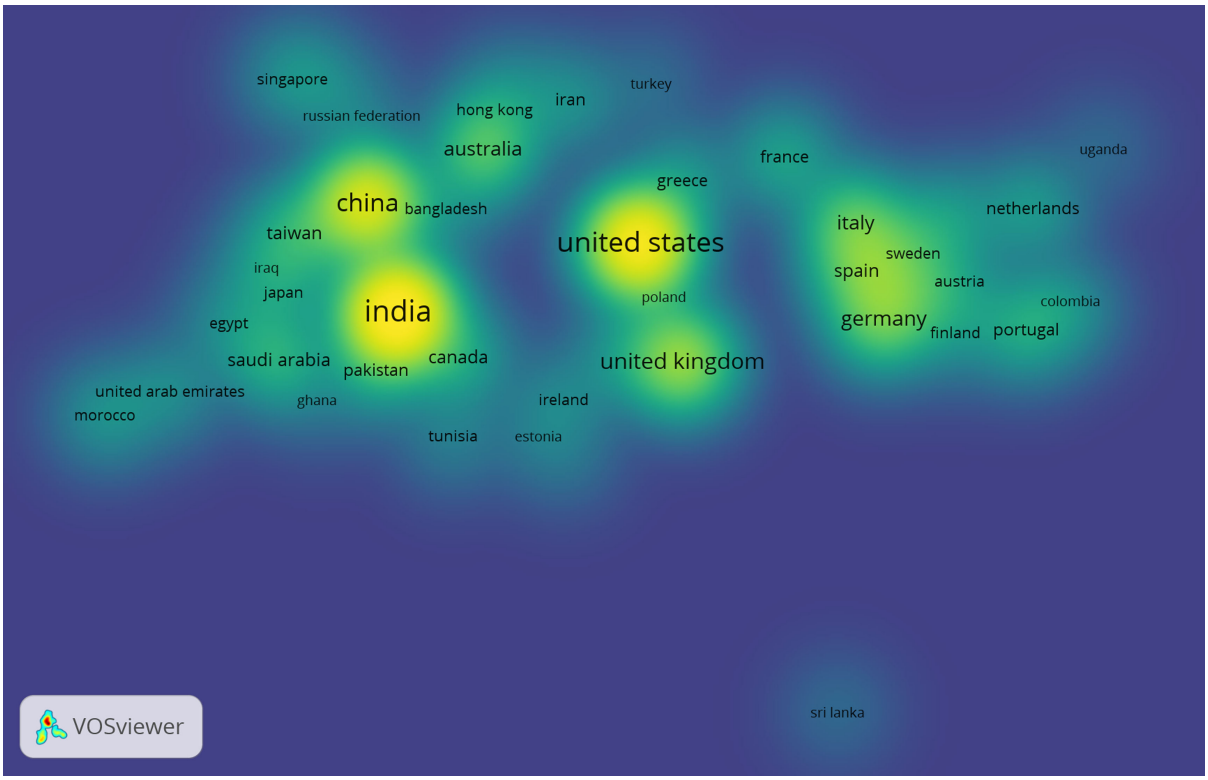

Figure 4
Literature review selection process

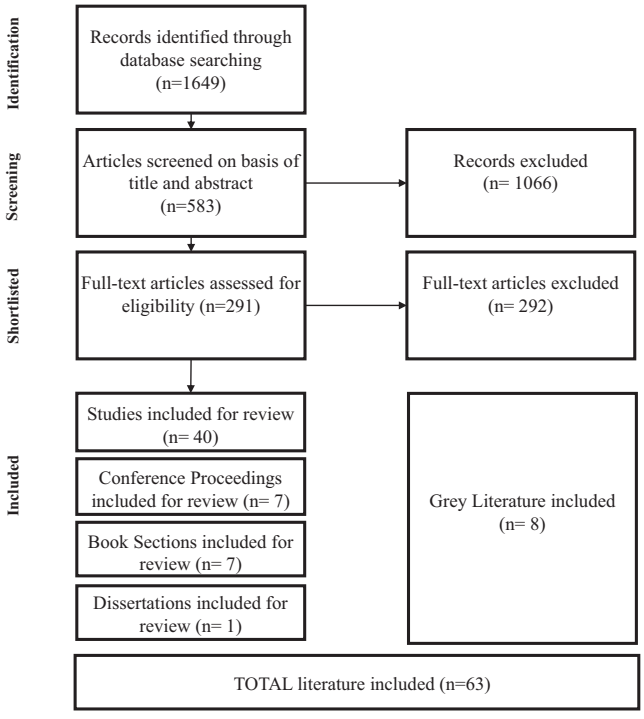

Figure 4 demonstrated the evaluation process followed while ensuring consistent quality assessment.

This systematic approach ensured a thorough and unbiased selection of 39 studies relevant to the research question, ultimately providing a robust foundation for the review's conclusions.

2.3. Data extraction and analysis

To extract the most important details about GDPR compliance in HMS, the data extraction procedure involves thoroughly going over the chosen articles and papers. The data that were extracted contained information on the difficulties encountered, mitigation techniques, necessary legal changes, market landscape and implications, GDPR compliance measures, challenges faced by HMS, strategies proposed or implemented, and future research directions. In order to ease the analysis and synthesis efforts, this material was organized in a manner that permits the identification of recurring themes, trends, and patterns, moreover, the retrieved information was categorized and synthesized during the data analysis process. A thorough review of GDPR compliance inside HMS was also the intent of this analysis, which further emphasized the significant results and insights from the literature. To guarantee the validity and reliability of the data acquired, strict quality control procedures were applied throughout the analysis.

2.4. Ethics

Conducting this study required careful attention to ethical issues. All of the data sources utilized in this study complied with

copyright and intellectual property laws and were openly accessible. To maintain academic integrity, the researchers made sure that the original authors and materials were properly cited and acknowledged.

2.5. Limitations

It is critical to recognize this methodology's limitations. It's probable that some important research or publications were overlooked due to the topic's breadth and the GDPR compliance's dynamic nature. However, by employing a thorough search technique and including a wide range of data sources, efforts were made to reduce the impact of this constraint on the research. In order to guarantee that the information acquired was current and relevant, the inclusion criteria concentrated on recently published works.

2.6. Study validation

The synthesis data was cross-checked with data from multiple sources to guarantee accuracy and consistency, in order to confirm the validity of the study findings. The consensus obtained during the review process served as the foundation for the conclusions made after the data analysis, which were also supported by the evidence gathered.

3. Literature Review

3.1. UAE healthcare

3.1.1. Healthcare infrastructure in the UAE

The healthcare infrastructure in the UAE has experienced impressive expansion and improvement. Modern healthcare facilities are being built with a lot of emphasis from the government, which makes the UAE a desirable location for medical tourism [5]. The nation is home to a large number of contemporary hospitals, specialty clinics, and medical facilities outfitted with cutting-edge infrastructure and technologies, making the country a medical tourism hub, providing locals and visitors from abroad with a wide range of healthcare facilities [6, 7].

3.1.2. Data protection and the regulatory framework

The UAE has enacted extensive legislation to safeguard the secure processing of personal data in healthcare settings, in accordance with the global shift toward data security and privacy. The UAE has established legal structures such as the NESA and laws such as the Federal Law No. 2 of 2019 on the Use of Information and Communication Technology in the Health Sector to protect personal information, even if it does not have a dedicated data protection law comparable to the European GDPR [8].

3.1.3. Compliance with GDPR and healthcare providers

In order to comply with GDPR rules, healthcare providers in the UAE are aggressively updating their systems and procedures. HMS must adhere to GDPR principles such as data minimization, purpose limitation, and lawful basis for processing because they handle patient data in a crucial way. Healthcare providers in the UAE are putting organizational and technical controls in place within their HMS to guarantee GDPR compliance. To properly monitor and protect personal data, these techniques include data encryption, pseudonymization, access limitations, and frequent data audits. Additionally, to manage GDPR compliance and guarantee continuous respect to data privacy laws, healthcare firms are recruiting Data Privacy Officers (DPOs). The UAE's involvement with international data protection bodies and organizations further demonstrates its dedication to GDPR compliance. The UAE Data Protection Committee works with international organizations to share best practices and raise data protection requirements in the nation's healthcare industry [9].

In the UAE, the principle of data minimization is becoming increasingly relevant as healthcare organizations strive to align with global data protection standards while respecting local regulations. With the UAE's focus on digital health initiatives, rigorous data audits within HMS are essential to identify and categorize personal data accurately. Applying data minimization techniques, such as pseudonymization and anonymization, helps reduce the risk of processing excessive personal data and enhances compliance with both GDPR and UAE-specific data protection requirements. Purpose limitation is equally crucial, ensuring that personal data are only used for lawful and predefined purposes. By establishing clear policies and procedures for data processing, UAE healthcare organizations can mitigate risks associated with non-compliance and align with the country's evolving legal landscape.

3.2. Hospital management systems and health data

3.2.1. Hospital management systems (HMS)

The effective and efficient provision of healthcare services is greatly facilitated by the use of robust HMS [10]. These systems include a wide range of hardware, programs, and procedures that make it possible to gather, handle, store, and analyze health-related data. Patient management, Electronic Health Records (EHRs), scheduling, billing, and decision support are just a few of the tasks that HMS support healthcare firms with its core processes [11].

HMS is defined as a system that includes computerized patient registration and retention of their medical profiles and information [12]. Access to this software is through restricted log-in details of dedicated employees to access patient records and add information through customized user interfaces. HMS covers a wide spectrum of administrative procedures, activity-based pricing, and reporting capability. The use of HMS enables clinical organizations to grow their business, enhances their caregiver's productivity and work quality, and simplifies all management processes inclusive of patient registration, diagnostics, consultation, discharge, and admission to name a few [13]. HMS efficiently and effectively connects all involved stakeholders in the patient journey eliminating silo operation and waste [14].

In the UAE, the rapid digital transformation of the healthcare sector is driving the adoption of advanced HMS. These systems are essential in integrating patient management, EHRs, and other core functions across a diverse and multicultural population. Given the UAE's focus on becoming a global leader in healthcare, HMS plays a crucial role in enhancing operational efficiency, improving patient outcomes, and supporting the country's vision of a world-class healthcare system. The integration of HMS with the UAE's national health information exchange (Riayati) also highlights the importance of interoperability and data sharing in the region's healthcare landscape.

3.2.2. The value of health information

Any hospital system would be incomplete without the vital information that health data provides regarding patients, diagnosis, treatments, and outcomes. This information comes from a wide variety of sources, including patient demographics, medical histories, lab results, imaging reports, and vital signs. Healthcare practitioners can improve care coordination, make educated

decisions post-diagnosis, and improve patient outcomes by utilizing health data inside HMS [15].

In the UAE, health information is a critical asset in achieving the government's vision of a fully integrated healthcare system that meets international standards. The accurate and timely management of health data within HMS is vital for improving patient care, enabling personalized treatments, and facilitating the country's ambitious public health initiatives. Health data are also instrumental in supporting the UAE's research and development efforts, driving innovation in healthcare services, and contributing to the nation's strategic goals of enhancing population health and healthcare sustainability.

3.2.3. Health data management challenges

Despite the enormous usefulness of health data, managing it effectively presents an array of difficulties. The sheer amount and complexity of health data produced by many healthcare stakeholders, such as hospitals, clinics, laboratories, and pharmacies, is a major concern. It might be challenging to integrate and harmonize this data within HMS; this requires safe data sharing channels and interoperability standards [16]. Furthermore, because health information is so sensitive, it must adhere to strict security and privacy rules. To adhere to laws like the GDPR, patient confidentiality and privacy must be protected. Strong security measures are necessary within HMS to protect health data from unwanted access, breaches, and misuse [17].

In the UAE, managing health data within HMS poses unique challenges due to the diverse population, rapid technological advancements, and the evolving regulatory landscape. The integration of data from various sources, including public and private healthcare providers, requires robust interoperability frameworks to ensure seamless data exchange. Moreover, with the absence of a comprehensive national data protection law equivalent to GDPR, healthcare organizations face uncertainties in ensuring patient privacy and data security. Addressing these challenges is critical for maintaining public trust and complying with emerging data protection regulations in the UAE.

3.2.4. Integration and interoperability

The handling of health data inside HMS must be interoperable. It speaks to the smooth interchange and utilization of health data between various systems, programs, and gadgets. Interoperability enables access to comprehensive patient data, fosters care coordination, and enhances decision-making for healthcare professionals. There are initiatives under progress to provide common frameworks and standards for the interoperability of health data. Health Level Seven International and Fast Healthcare Interoperability Resources (FHIR) are two projects that seek to standardize data formats and protocols to enable easy data interchange across various HMS and healthcare organizations (*FHIR*). The undergone effort demonstrates that there is work still to be conducted to ensure compliance to GDPR standards around interchange and utilization of health data [18].

The UAE's healthcare sector recognizes the critical importance of interoperability in HMS to ensure seamless access to patient data across different healthcare providers [19]. Initiatives such as the Riayati national health information exchange aim to standardize data formats and protocols, facilitating the smooth exchange of health information across various HMS [20]. However, ensuring compliance with global standards like GDPR remains a challenge, necessitating further efforts to develop region-specific frameworks that support both interoperability and data protection in the UAE's unique healthcare environment.

3.2.5. Security and privacy in the management of health data

When designing and implementing an HMS, security and privacy of patient data are crucial factors to consider. Some of the technical safeguards used by HMS to protect health data include data encryption, access limits, user authentication, and audit trails. The lawful and moral use of health data is also guaranteed by strong data governance policies, consent management systems, and respect to privacy laws [21]. The implementation of thorough data breach response strategies by HMS is also required, including prompt communication of affected parties and regulatory authorities in the event of a breach. To ensure GDPR compliance and protect patient privacy, data protection impact assessments (DPIAs) can help identify potential risks and mitigation options [22].

In the UAE, ensuring the security and privacy of health data within HMS is a top priority, particularly as the country embraces digital health initiatives. The UAE's healthcare organizations are increasingly adopting advanced security measures such as data encryption, access controls, and user authentication to protect patient data. However, the lack of a unified national data protection framework similar to GDPR presents challenges in maintaining consistent data governance and privacy practices [23]. To address these issues, UAE healthcare providers are encouraged to conduct regular DPIAs and implement comprehensive data breach response plans to safeguard patient information and build public trust.

3.2.6. Advantages of efficient health data management

Numerous advantages result from the efficient management of health data within the HMS. Access to complete and accurate patient data allows healthcare professionals to make better diagnoses, customize treatments, and enhance patient outcomes [24]. HMS's data analytics and decision support capabilities support clinical research, population health management, and evidence-based care. Additionally, effective administration of health data lowers administrative burden, simplifies procedures, and improves operational efficiency within healthcare companies [25].

Efficient management of health data within HMS in the UAE offers significant benefits, aligning with the country's vision for a high-performing healthcare system [5]. By providing healthcare professionals with accurate and comprehensive patient data, HMS enables more precise diagnoses, personalized treatments, and improved patient outcomes. Additionally, the ability to analyze health data supports the UAE's goals of advancing clinical research, optimizing population health management, and enhancing operational efficiency. These advantages are crucial for positioning the UAE as a leader in healthcare innovation and for meeting the growing demands of its diverse population [26].

3.3. General data protection regulation (GDPR)

According to the GDPR Compliance Guide published by [27], GDPR is the toughest privacy and security law across the globe imposing obligations onto any organization (inclusive healthcare) in any country collecting data related to people in the EU. Since May 25 2028, GDPR has been charging substantial fines (up to €20 million) against any violators to its standards. Since May 25, 2018, the GDPR has imposed significant fines of up to €20 million on any organizations that violate its standards. The regulation applies to any service or product offered to EU citizens

or residents, regardless of whether the organization is licensed or operates within the EU.

The GDPR identifies several types of data that require protection, each with its own set of challenges. These include personal data, sensitive personal data, genetic data, biometric data, and data related to criminal convictions or offenses. Personal data encompasses any information that can directly or indirectly identify an individual, such as names, addresses, and contact information. The protection challenge here lies in the broad scope of what constitutes personal data, requiring robust safeguards to prevent unauthorized access and misuse. Sensitive personal data includes information about racial or ethnic origin, political opinions, religious beliefs, and health-related data. The challenge with this type lies in the heightened risk of harm from breaches, necessitating stricter security measures. Genetic and biometric data, which are unique to an individual, pose significant challenges in maintaining privacy, particularly as this data is increasingly used in healthcare and security applications. Data related to criminal convictions or offenses is also highly sensitive, with stringent requirements for protection due to the potential for significant personal and societal impact if mishandled. Each type of GDPR data presents unique protection challenges, underscoring the need for tailored security measures and compliance strategies to safeguard individuals' privacy effectively [28, 29].

3.4. Compliance to GDPR in the UAE-based HMS

Article 35 of the GDPR Compliance Guard defined personal health data as "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test". [27]

This was further confirmed by the European Data Protection Supervisor who quoted: "The GDPR recognizes data concerning health as a special category of data and provides a definition for health data for data protection purposes. Though the innovative principles introduced by the GDPR (privacy by design or the prohibition of discriminatory profiling) remain relevant and applicable to health data as well, specific safeguards for personal health data and for a definitive interpretation of the rules that allows an effective and comprehensive protection of such data have now been addressed by the GDPR. Processes that foster innovation and better-quality healthcare, such as clinical trials or mobile health, need robust data protection safeguards in order to maintain the trust and confidence of individuals in the rules designed to protect their data" [30].

Many clinical operators in the UAE market rely on the regulator's standards (such as the policy on the Abu Dhabi Health Information Exchange, DHA Health Data Protection and Confidentiality Policy) that are derived from Health Insurance Portability and Accountability Act of 1996 (HIPAA) standards which is focused on healthcare organizations and the manner by which personal health information is used. Despite it being focused on hospital operators in the US, many healthcare providers adopt its standards which is a challenge given that GDPR is a ***broader*** legislation that supervises any organization that handles personal information of an EU or UK citizen when provisioning its service portfolio. Similarities between HIPAA and GDPR Compliance are that both require [31]:

1) Controlled access to sensitive data
2) Detecting unauthorized changes to PHI
3) PHI encryption at rest and in transit
4) An appointed DPO
5) Healthcare providers to focus on the security of their clients, patients, and employees' privacy [32] pointed the difference between HIPAA and GDPR Compliance which indicates that the UAE-based hospitals need to close this gap as outlined in Table 2.

Table 2
Difference between HIPAA and GDPR compliance

Areas	HIPAA	GDPR
Consent	HIPAA permits some degree of PHI disclosure without patient consent. For example, healthcare providers can send PHI to another provider for treatment purposes. In some circumstances, a healthcare provider can disclose PHI to other providers or business associates without patient consent.	Under GDPR, however, consent must always be given, even for patient care.
Right to be forgotten	Under HIPAA, medical records and other personal information can't be altered or deleted. In other words, although subject to privacy, the information is stored forever.	GDPR gives data subjects the right to be forgotten, where individuals have the right to tell an organization to erase their data.
Data breaches	Under the HIPAA breach notification rule, covered entities, and business associates must notify affected individuals of breaches. If the incident involves over 500 individuals, the organization must notify the OCR and all affected individuals within 60 days.	With the GDPR, breach size does not matter. Article 33 of the GDPR places a 72-hour breach reporting deadline and requires providers to report all breaches to supervisory authorities.

Despite the February 2019, Federal Law No 2 of 2019 (Health Data Law) which regulates the use of information technology and communications in the healthcare sector. Despite the enactment of Federal Law No. 2 of 2019 (Health Data Law) in February 2019, which regulates the use of information technology and communications in the healthcare sector, the identified gaps remain unaddressed. There is a need to strengthen controls to ensure full compliance with GDPR.

3.5. Proposed mitigation solutions

Limiting the amount of personal data that is collected and processed for certain purposes is known as "data minimization" or "purpose limitation". Healthcare organizations can do this by doing rigorous data audits to identify and categorize the different sorts of data that are gathered and maintained inside their HMS. The danger of processing too much personal data can be decreased by applying data minimization techniques like pseudonymization and anonymization, which will improve GDPR compliance. The goal of purpose limitation is to make sure that personal data are only used for legal and predetermined purposes. The legal justification for processing personal data inside an HMS should be made clear in policies and procedures established by healthcare organizations. Risks associated with non-compliance can be reduced by putting in place procedures to monitor and enforce purpose limitation, such as access controls and periodic assessments [32].

Integrating privacy by design and default concepts into the creation and administration of HMS is essential for GDPR compliance. Consideration of privacy and data protection issues at the outset of system design is known as privacy by design. In the UAE's rapidly growing healthcare sector, integrating privacy by design and default into the development and management of HMS is vital for both GDPR compliance and adherence to local privacy regulations. As the UAE advances its digital health initiatives, healthcare organizations must prioritize privacy and data protection from the outset of system design. Conducting privacy impact Assessments (PIAs) helps identify potential privacy issues, enabling the incorporation of privacy-enhancing technologies (PETs) such as encryption, data anonymization, and granular consent processes into HMS. Privacy by default ensures that HMS is configured with the highest level of privacy protection from the start, restricting access to personal data to authorized individuals only. By embracing these principles, UAE healthcare organizations can proactively address privacy risks and meet both international and local data protection obligations [33].

Furthermore, organizations in the healthcare industry should use PIAs to identify potential privacy issues and create suitable measures [34]. For example, granular permission processes, encryption, and data anonymization are PETs and features that can be incorporated into HMS. Privacy by default makes sure that HMS is set up with the maximum level of privacy protection by default. Reviewing and configuring system settings to prioritize privacy and restrict access to personal data to authorized individuals only is a good idea for healthcare businesses. Organizations in the healthcare industry can proactively address GDPR obligations and reduce privacy risks by implementing privacy by design and default principles [35].

3.5.1. Data subject rights and consent management

The GDPR gives people particular rights to their personal information, including the ability to view, correct, erase, and limit how that information is processed [36].To make it simple for people to exercise their rights, healthcare organizations should set up reliable routines and procedures inside HMS [37]. This could entail setting up self-service portals or user interfaces that let people manage their consent preferences and successfully exercise their rights. The management of consent is essential to GDPR compliance. The processing of personal data by healthcare organizations should only occur with the express and informed agreement of the data subject. This includes describing the goals, scope, and timeframe of data processing tasks in explicit terms. Mechanisms for obtaining and managing consent should be made available by HMS, including alternatives for withdrawal and routine consent renewal [38].

In the UAE, respecting data subject rights is essential as the country aligns with global data protection practices, including GDPR principles. Healthcare organizations must implement robust processes within HMS to facilitate the exercise of data subject rights, such as access, correction, and erasure of personal information. In a region where patient trust is paramount, establishing user-friendly self-service portals and interfaces that allow individuals to manage their consent preferences is critical. Consent management is a key aspect of GDPR compliance and is increasingly relevant in the UAE's healthcare landscape. HMS should ensure that personal data is processed only with the explicit and informed consent of the data subject, clearly defining the purpose, scope, and duration of data processing activities. Providing mechanisms for consent withdrawal and regular renewal further strengthens compliance and patient trust in the UAE.

3.5.2. Data breach detection and notification

The security and privacy of personal data are seriously threatened by data breaches. This requires healthcare organizations to implement robust safeguards within the HMS to quickly detect, address, and mitigate data breaches. This entails closely monitoring system logs, placing robust intrusion detection systems, and regularly performing vulnerability assessments. Healthcare businesses should have clear protocols in place to notify impacted persons and the appropriate supervisory authorities in the case of a data breach, as mandated by GDPR. For prompt and legal reporting, it is essential that the HMS supports automated breach notification procedures [39].

In the UAE, where healthcare data security is a top priority, the ability to detect and respond to data breaches within HMS is critical [39]. Given the region's emphasis on maintaining high standards of data protection, healthcare organizations must implement strong safeguards, including continuous monitoring of system logs, robust intrusion detection systems, and regular vulnerability assessments [40]. The UAE's legal framework is evolving to address data protection, making it essential for healthcare providers to have clear protocols for breach detection and notification. In line with GDPR requirements, UAE healthcare organizations must ensure that their HMS supports automated breach notification procedures, enabling prompt reporting to affected individuals and relevant authorities. This proactive approach is vital for maintaining patient trust and ensuring compliance with both international and local data protection regulations.

3.6. Legislative change required

A precise definition of health data is necessary to understand its importance and the need for special protection. Legislative frameworks must, however, provide explicit and detailed definitions of health data. This involves outlining precisely what counts as health information, such as medical histories, treatment logs, genetic data, or information on mental health. Healthcare companies will be able to correctly identify and handle health data within their HMS through the use of clear definitions [41].

3.6.1. Harmonization of national laws with GDPR

National laws pertaining to data protection and healthcare should be in line with the provisions of GDPR in order to achieve consistency and harmonization. Healthcare data privacy rules may vary from those required by the GDPR in some countries. Healthcare firms will be able to streamline their compliance processes and reduce misunderstanding when operating in many jurisdictions by harmonizing these laws [42].

3.6.2. Strengthening consent requirements

Obtaining consent is an essential part of complying with GDPR. Legislative reforms, however, are required to tighten the standards for getting valid consent for the processing of health data inside HMS. The requirement of explicit and informed consent, the capacity to withdraw consent, and the scope and duration of data processing activities should all be governed by clear rules. Legislative amendments should consider unique rules for delicate categories of health data, like genetic or biometric data [43].

3.6.3. Improved cross-border data transfer methodologies

Cross-border data transfers are frequent in the healthcare industry, particularly when working with foreign healthcare providers or carrying out medical research. To create reliable systems for the legal movement of health data between jurisdictions while maintaining GDPR compliance, legislative adjustments are necessary. To establish a legal foundation for cross-border data transfers, these mechanisms should include precise specifications for data transfer agreements, typical contractual provisions, or binding corporate norms [44].

3.6.4. Streamlining research and public health expectations

Research and public health initiatives frequently use personal data, including health information, for uses including disease surveillance, public health interventions, and medical research. Legislative amendments should include unequivocal and clear exceptions or derogations that permit the GDPR-compliant processing of health data for research and public health objectives. The protection of individual rights and the facilitation of significant research and public health activities should both be balanced by these exceptions [45].

3.6.5. Effective enforcement mechanism and adequate fines

To guarantee GDPR compliance in the healthcare sector, effective enforcement mechanisms and adequate fines are crucial. Legislative amendments should close any loopholes in the enforcement system, including the creation of capable supervisory authorities with enough authority and resources to oversee GDPR compliance. Healthcare organizations should be encouraged to prioritize data protection procedures within their HMS by fair and deterrent penalties for non-compliance [46].

3.7. Market landscape and implications

HMS and the larger healthcare market have experienced major effects as a result of the GDPR's introduction. The market implications that have resulted from GDPR compliance activities within the healthcare sector are examined in this section [47].

3.7.1. Increased focus on data protection

The healthcare industry is now paying more attention to and emphasizing data protection as a result of GDPR. Healthcare firms have taken proactive steps to comply with GDPR rules because they understand how important it is to protect patient data. This entails putting in place strong security measures, adopting technologies that enhance privacy, and improving data governance processes inside their HMS. Patients now have more trust and confidence thanks to the increased focus on data protection, which has increased patient loyalty and happiness [48].

3.7.2. Evolution of data-driven healthcare

Healthcare firms have reviewed their data management and analytics strategies in response to GDPR compliance. Organizations have grown more cautious about how they acquire, retain, and use health data within their HMS as a result of tightening restrictions surrounding permission and data usage. As a result, there is now a greater emphasis on gaining informed consent, guaranteeing data accuracy, and preserving patient privacy in data-driven healthcare. In order to improve clinical outcomes and tailor patient care, healthcare practitioners are using data analytics in a more moral and transparent manner [49].

3.7.3. Emergence of PETs

Healthcare organizations have integrated PETs within their HMS to satisfy GDPR compliance standards. Through the use of PETs like differential privacy, secure multiparty computation, and homomorphic encryption, businesses may safeguard patient data while gaining insightful information. These technologies make it possible to collaborate and share data without jeopardizing people's privacy. In addition to making GDPR compliance easier, the rise of PETs has stimulated healthcare market innovation and opened doors for the creation of cutting-edge security and privacy solutions [50].

3.7.4. Growing importance of data governance

The need for effective data governance procedures in the healthcare industry has been highlighted by GDPR compliance. Clear rules, procedures, and accountability structures are necessary for healthcare organizations to ensure the proper management and security of personal data inside their HMS. This led to the creation of specialized data governance teams, the selection of Data Protection Officers (DPOs), and the adoption of GDPR-compliant data governance frameworks. The quality, integrity, and accessibility of data have been improved through greater data governance, which has improved decision-making, shortened processes, and improved patient outcomes [51].

3.7.5. Impact on medical research and innovation

The healthcare industry's ability to comply with GDPR has ramifications for medical research and innovation. For research institutions and businesses engaged in extensive data analytics projects, the GDPR's regulations for consent and data usage have presented difficulties. A balance between data privacy and assisting medical research is being sought, nevertheless. In order to ensure that research projects adhere to GDPR while fostering

creative, society-beneficial research, ethical review boards and research ethics committees are essential. Compliance with GDPR has sparked the creation of data sharing frameworks and partnerships that place a priority on patient privacy and permission, encouraging ethical and open research practices [52].

4. Conclusion

A thorough framework for data protection and privacy in the healthcare industry has been implemented by the GDPR. This article provided a thorough analysis of GDPR compliance inside HMS, looking at the difficulties encountered, potential mitigation measures, necessary legislative changes, market results, and future research prospects. This study made it clear that obtaining GDPR compliance in HMS is a difficult task with many moving parts. Healthcare firms must deal with issues such as managing consent, data subject rights, data breach management, third-party vendor management, and cross-border data transfers, as well as the complexity and ambiguity of GDPR rules. To assure compliance while safeguarding patients' privacy and data rights, these difficulties demand a comprehensive strategy comprising strong systems, rules, and procedures. To deal with these issues, suggested mitigation measures have been found. Implementing privacy by design principles, performing extensive DPIAs, improving consent management procedures, bolstering data breach detection and response mechanisms, setting up efficient vendor management procedures, and ensuring secure cross-border data transfers are a few of these. A legislative overhaul is also necessary to improve HMS compliance with GDPR. The goal of these modifications should be to give clearer instructions and interpretations of GDPR rules that are relevant to the healthcare industry. Additionally, in order to create industry-specific standards and best practices that comply with GDPR rules, regulatory bodies must collaborate closely with healthcare firms. The adoption of GDPR in HMS has had a tremendous impact on the market. In order to comply, healthcare institutions have made investments in staff training, PETs, and data protection procedures. Patients now have more control over their personal information, which has improved the confidence and transparency in the healthcare industry. A market for products that can help healthcare businesses fulfill their requirements has also been created as a result of GDPR compliance's encouragement of innovation in data security and privacy technology. Despite the advancements, there are still a number of directions in which further research on GDPR compliance inside HMS might go. Future research might examine the effectiveness of mitigation strategies that have been suggested, the effects of GDPR on patient satisfaction and healthcare outcomes, the investigation of ethical issues related to data processing, and the creation of standardized frameworks for data protection in healthcare.

In summary, the GDPR significantly impacts HMS by imposing stringent compliance requirements and data protection practices [4]. HMS must ensure robust mechanisms for securing personal data, including implementing strong encryption, access controls, and audit trails to protect patient information. GDPR mandates clear procedures for obtaining explicit consent, managing data subject rights, and handling data breaches, which necessitates comprehensive data governance and privacy policies. Additionally, HMS must support data minimization and purpose limitation principles, ensuring that data is collected and processed only for legitimate purposes. Compliance with GDPR also requires regular DPIAs and adherence to cross-border data transfer regulations, driving hospitals to adopt advanced technologies and practices to safeguard patient privacy and avoid significant penalties.

The impact of GDPR on HMS aligns with previous research that highlights the regulation's emphasis on robust data protection practices and compliance requirements. Studies have shown that GDPR drives significant changes in how HMS manage personal data, necessitating enhanced security measures such as encryption and access controls to protect patient information. Research also underscores the importance of implementing comprehensive consent management and data subject rights processes, as well as conducting regular DPIAs. Additionally, literature emphasizes the need for HMS to adhere to principles of data minimization and purpose limitation to comply with GDPR. Overall, previous research supports the view that GDPR introduces rigorous standards that compel healthcare organizations to adopt advanced data protection practices and technologies to ensure compliance and safeguard patient privacy [28].

5. Future Areas of Research

The GDPR has established a strong foundation for data protection and privacy in HMS. However, there are still some topics that need for additional study and investigation in order to improve GDPR compliance and handle new problems. This section identifies possible research directions in the context of HMS GDPR compliance [52].

5.1. Impact of technological advancements

Blockchain, machine learning, and artificial intelligence (AI) have the potential to revolutionize data management and healthcare delivery. Future studies could look into how these technologies affect HMS's ability to comply with GDPR. It also entails exploring the use of blockchain for secure and transparent data sharing, comprehending how AI and ML algorithms can be developed to respect privacy and data protection requirements, and evaluating the potential risks and benefits of these technologies in the context of GDPR [53].

5.2. Evaluation of GDPR implementation effectiveness

As GDPR compliance initiatives develop, it is essential to assess how well they work in actual healthcare settings. Future studies can examine how GDPR affects data protection procedures, patient outcomes, and organizational effectiveness. This entails carrying out thorough audits and evaluations to gauge the degree of compliance, finding gaps and potential development areas, and evaluating the overall advantages and difficulties of implementing GDPR within HMS. The COVID-19 epidemic has pushed the use of telehealth services, which entail the collecting and processing of private patient data remotely. Future studies can examine the particular difficulties and factors involved in GDPR compliance in telehealth settings. In order to achieve GDPR compliance in telehealth activities, this may entail assessing the efficiency of current security measures in safeguarding patient data during remote consultations, identifying potential vulnerabilities and privacy issues, and providing mitigation methods [54].

5.3. Ethical considerations in data sharing

Data sharing is essential for teamwork and research in the field of medicine. The ethical issues of data sharing under the constraints of GDPR can be explored in future research. This entails examining

the moral ramifications of sharing de-identified or pseudonymized data, being aware of the difficulties in obtaining informed consent for data sharing and assessing the GDPR's potential impact on data sharing practices for public health and medical research projects [55].

5.4. Data transfers across borders and international compliance

In the healthcare industry where international collaborations are frequent, the movement of personal data across national boundaries continues to be a challenging problem. In the context of cross-border data transfers, future research can concentrate on comprehending the difficulties and investigating viable solutions for GDPR compliance. This entails evaluating the effectiveness of the current data transfer systems, determining how international data protection laws will affect healthcare companies, and suggesting methods for achieving smooth and legal cross-border data flows [56].

Our findings may lead to the adoption of advanced security measures, such as encryption and pseudonymization, within HMS to protect sensitive patient data [57]. It may encourage the development of patient-centered data protection models, where patients have more control over their data, aligning with GDPR's principles [58].

5.5. Long-term effects of GDPR on healthcare innovation

GDPR compliance may have an impact on the advancement of cutting-edge medical innovations. Future studies can look into the GDPR's long-term effects on medical innovation and the adoption of new technology. This entails determining how to strike a balance between data security and innovation, comprehending how GDPR rules may be included into the design and development of new medical technologies, and coming up with ways to encourage a culture of privacy and innovation within the healthcare industry [59].

Future research could explore comparative studies between GDPR and other data protection regulations globally which could be an important area for future research, aiding in the development of global data protection standards [60]. There may be a need for longitudinal quantitative studies to assess the long-term effects of GDPR compliance on healthcare organizations, particularly regarding patient data protection and trust [61].

5.6. Variability in GDPR implementation and strategies

The variability in GDPR implementation across different healthcare settings could be a key area for future investigation [62]. Our paper's findings could also guide healthcare organizations in refining their GDPR compliance strategies, emphasizing the importance of robust data governance and risk management practices [63]. Moreover, it underlines the importance of regular training for healthcare staff on GDPR requirements, which could be critical for maintaining compliance [64].

6. Theoretical and Practical Contributions

Despite limitations, our research contributes to current discussions on contextualized research. Through this SLR we attempted to establish a foundation to identify the existing studies from the context-emic perspective. By encouraging the research community to "optimal allocation of effort between exploitation and exploration", looking at theoretical contributions from the periphery will progress management and organization science [65]. We encourage academics to perform empirical studies for the benefit of advancing literature in this arena. From a practical contribution, this research could be used by EHR Information Technology specialists, IT architects, hospital executive management members when designing their EMR and cater to what would be feasible for their operational environments and the need of their employees. Furthermore, academics in the field of information technology, hospital management, and EMR vendors will benefit from this systematic review as it allows them to build on the existing relevant literature.

Also, our review could inform policymakers about the specific needs of healthcare organizations regarding GDPR compliance, potentially leading to more tailored regulations [66]. It contributes to standardizing GDPR compliance practices across healthcare systems, ensuring a consistent approach to data protection [67].

Glossary

- **GDPR**: General Data Protection Regulation is the privacy and security law across the globe imposing obligations onto any organization (inclusive healthcare) in any country collecting data related to people in the EU.
- **HMS**: Hospital Management Systems includes a wide range of hardware, programs, and procedures that make it possible to gather, handle, store, and analyze health-related data.
- **NESA**: The National Electronic Security Authority in the UAE, offers rules and regulations for the security of sensitive data, including health information.
- **Data Encryption**: Is the process of converting plaintext into a coded form (ciphertext) to prevent unauthorized access to the patient's health information.
- **Pseudonymization**: is the technique of replacing private identifiers in data with pseudonyms or fictitious identifiers, thereby protecting personal information while allowing patient data processing.
- **Access Limitations**: are restrictions placed on who can view, modify, or interact with patient health data, ensuring that only authorized individuals or systems have the necessary permissions to access specific information.
- **Patient Data Audits**: are systematic reviews and examinations of how patient information is accessed, used, stored, and shared within a healthcare system to ensure compliance with legal, regulatory, and organizational standards for data privacy and security.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Inas Al Khatib: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft, Visualization, Project administration. **Norhan Ahmed:** Methodology, Formal analysis, Writing – original draft, Supervision, Funding acquisition, Project administration. **Malick Ndyiaye:** Writing – review & editing, Supervision.

References

[1] Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. *Journal of Big Data*, *3*(25), 1–25. https://doi.org/10.1186/s40537-016-0059-y

[2] Hoofnagle, C. J., Sloot, B. V., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

[3] Amini, M. M., Jesus, M., Sheikholeslami, D. F., Alves, P., Benam, A. H., & Hariri, F. (2023). Artificial intelligence ethics and challenges in healthcare applications: A comprehensive review in the context of the European GDPR mandate. *Machine Learning and Knowledge Extraction*, *5*(3), 1023–1035. https://doi.org/10.3390/make5030053

[4] Yuan, B., & Li, J. (2019). The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the European Union: An empirical investigation. *International Journal of Environmental Research and Public Health*, *16*(6), 1070. https://doi.org/10.3390/ijerph16061070

[5] Koornneef, E., Robben, P., & Blair, I. (2017). Progress and outcomes of health systems reform in the United Arab Emirates: A systematic review. *BMC Health Services Research*, *17*(1), 672. https://doi.org/10.1186/s12913-017-2597-1

[6] Al-Talabani, H., Kilic, H., Ozturen, A., & Qasim, S. O. (2019). Advancing medical tourism in the United Arab Emirates: Toward a sustainable health care system. *Sustainability*, *11*(1), 230. https://doi.org/10.3390/su11010230

[7] Ahmed, G., Amiri, N. A., & Khan, W. (2018). Outward medical tourism: A case of UAE. *Theoretical Economics Letters*, *8*(7), 1368–1390. https://doi.org/10.4236/tel.2018.87088

[8] Sarabdeen, J., & Moonesar, I. A. (2018). Privacy protection laws and public perception of data privacy: The case of Dubai e-health care services. *Benchmarking: An International Journal*, *25*(6), 1883–1902.

[9] Albejaidi, F. M. (2010). Healthcare system in Saudi Arabia: An analysis of structure, total quality management and future challenges. *Journal of Alternative Perspectives in the Social Sciences*, *2*(2), 794–818.

[10] Junaid, S. B., Imam, A. A., Balogun, A. O., Silva, L. C., Surakat, Y. A., Kumar, G., . . . , & Mahamad, S. (2022). Recent advancements in emerging technologies for healthcare management systems: A survey. *Healthcare*, *10*(10), 1–45. https://doi.org/10.3390/healthcare10101940

[11] Rajamani, S. K., & Iyer, R. S. (2023). Networks in healthcare: A systematic review. *BioMedInformatics*, *3*(2), 391–404. https://doi.org/10.3390/biomedinformatics3020026

[12] Nishanthan, K., Mathyvathana, S., Priyanthi, R., Thusara, A., De Silva, D., & Cooray, D. (2022). The hospital management system. *International Journal of Engineering and Management Research*, *12*(5), 135–149.

[13] Génesis, C. A., Stefania, G. C., Karen, P. J., Claudia, G. D., & Yulineth, G. C. (2022). Occupational safety and health management systems as a component of labor productivity. *Procedia Computer Science*, *203*, 667–672.

[14] Pillay, R. (2023). Digital health trends. In A. Meyers (Ed.), *Digital health entrepreneurship. Health informatics* (pp. 123–129). Springer. https://doi.org/10.1007/978-3-031-33902-8_10

[15] Schmidt, M., Schmidt, S. A., Adelborg, K., Sundbøll, J., Laugesen, K., Ehrenstein, V., & Sørensen, H. T. (2019). The Danish health care system and epidemiological research: From health care contacts to database records. *Clinical Epidemiology*, *12*(11), 563–591. https://doi.org/10.2147/CLEP.S179083

[16] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems*, *2*, 1–10.

[17] Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: A systematic mapping study. *Journal of Public Health*, *32*, 435–454. https://doi.org/10.1007/s10389-022-01795-z

[18] Benson, T., & Grieve, G. (2021). *Principles of health interoperability: FHIR, HL7 and SNOMED CT*. Switzerland: Springer International Publishing AG.

[19] Khatiwada, A. P., Shrestha, S., Dharel, D., & Sapkota, B. (2023). Immunization practice in low and middle-income countries. In Z. U. D. Babar (Ed.), *Encyclopedia of evidence in pharmaceutical public health and health services research in pharmacy* (pp. 851–918). Springer International Publishing. https://doi.org/10.1007/978-3-030-64477-2

[20] Suryawanshi, P. B., & Aher, V. N. (2023). Analyse the various marketing strategies of healthcare insurance companies working in UAE. *International Journal of Professional Studies*, *15*, 1–8.

[21] Miller, A. R. (2024). Privacy of digital health information. In A. R. Miller, A. Goldfarb & C. E. Tucker (Eds.), *The economics of privacy* (pp. 127–162). University of Chicago Press. https://doi.org/10.7208/chicago/9780226834085-009

[22] Chudzynski, R. (2019). *EU general data protection regulation: Applicability to the Middle East*. UAE: PWC Middle East.

[23] Jones, M. C., Stone, T., Mason, S. M., Eames, A., & Franklin, M. (2023). Navigating data governance associated with real-world data for public benefit: An overview in the UK and future considerations. *BMJ Open*, *13*(10), 1–9. https://doi.org/10.1136/bmjopen-2022-069925

[24] Deokar, S., Mangla, M., & Akhare, R. (2021). A secure fog computing architecture for continuous health monitoring. In S. Tanwar (Ed.), *Fog computing for healthcare 4.0 environments: Technical, societal, and future implications* (pp. 269–290). Springer International Publishing AG.

[25] Kazadi, J. (2024). Data science and analytics in healthcare. *Data Science and Society Seminar*, 1–11. https://doi.org/10.13140/RG.2.2.25080.25608

[26] Alhajaj, K. E., & Moonesar, I. A. (2023). The power of big data mining to improve the health care system in the United Arab Emirates. *Journal of Big Data*, *10*(1), 1–33. https://doi.org/10.1186/s40537-022-00681-5

[27] GDPR EU. (2023). *Complete guide to GDPR compliance*. Retrieved from: https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

[28] Voigt, P., & Bussche, A. V. (2017). *The EU general data protection regulation (GDPR)*. USA: Springer. https://doi.org/10.1007/978-3-319-57959-7

[29] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). *The EU general data protection regulation (GDPR): A commentary get access arrow*. USA: Oxford Academic. https://doi.org/10.1093/oso/9780198826491.001.0001

[30] EDPS Europe. (2023). *Health*. Retrieved from: https://edps.europa.eu/data-protection/our-work/subjects/health_en

[31] OneTrust. (2022). *HIPAA vs. GDPR compliance: What's the difference?* Retrieved from: https://www.onetrust.com/blog/hipaa-vs-gdpr-compliance/#:~:text=HIPAA%20is%20focused%20on%20healthcare,an%20EU%20or%20UK%20citizen

[32] Forgó, N., Hänold, S., & Schütze, B. (2017). The principle of purpose limitation and big data. *New Technology, Big Data and the Law*, 17–42.

[33] Semantha, F. H., Azam, S., Shanmugam, B., & Yeo, K. C. (2023). PbDinEHR: A novel privacy by design developed framework using distributed data storage and sharing for secure and scalable electronic health records management. *Journal of Sensor and Actuator Networks*, *12*(2), 36.

[34] Kurtz, C., Semmann, M., & Böhmann, T. (2018). Privacy by design to comply with GDPR: A review on third-party data processors. In *Twenty-fourth Americas Conference on Information Systems.*

[35] Padyab, A., & Ståhlbröst, A. (2017). Privacy enhancing tools: A literature review on end-user role and evaluation. In *11th International Symposium on Human Aspects of Information Security & Assurance,* 28–30.

[36] Mantelero, A. (2013). The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

[37] Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), tyy001.

[38] Liddell, K., Simon, D. A., & Lucassen, A. (2021). Patient data ownership: Who owns your health? *Journal of Law and the Biosciences*, *8*(2), 1–50. https://doi.org/10.1093/jlb/lsab023

[39] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

[40] Boopathi, S. (2023). Securing healthcare systems integrated with IoT: Fundamentals, applications, and future trends. In *Dynamics of Swarm Intelligence Health Analysis for the Next Generation*, 86–209.

[41] Xafis, V., Schaefer, G. O., Labude, M. K., Brassington, I., Ballantyne, A., Lim, H. Y., . . . , & Tai, E. S. (2019). An ethics framework for big data in health and research. *Asian Bioethics Review*, *11*, 227–254.

[42] Shabani, M., & Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU general data protection regulation. *European Journal of Human Genetics*, *26*(2), 149–156.

[43] Shuaib, M., Alam, S., Alam, M. S., & Nasir, M. S. (2021). Compliance with HIPAA and GDPR in blockchain-based electronic health record. *Materials Today: Proceedings*.

[44] Verra, S. E., Kroeze, R., & Ruggeri, K. (2016). Facilitating safe and successful cross-border healthcare in the European Union. *Health Policy*, *120*(6), 718–727.

[45] Gennet, É. (2019). *Common infrastructure for national cohorts in Europe, Canada, and Africa (CINECA)-catalogue of ELSI issues*. Doctoral Dissertation.

[46] Georgiou, D., & Lambrinoudakis, C. (2020). GDPR compliance: Proposed guidelines for cloud-based health organizations. In *Computer Security: ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT*, 156–169.

[47] Semantha, F. H., Azam, S., Shanmugam, B., Yeo, K. C., & Beeravolu, A. R. (2021). A conceptual framework to ensure privacy in patient record management system. *IEEE Access*, *9*, 165667–165689.

[48] Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A process for data protection impact assessment under the European general data protection regulation. In *Privacy Technologies and Policy: 4th Annual Privacy Forum*, 21–37.

[49] Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Computer Law & Security Review*, *44*, 105640. https://doi.org/10.1016/j.clsr.2021.105640

[50] Becher, S., Gerl, A., Meier, B., & Bölz, F. (2020). Big picture on privacy enhancing technologies in e-health: A holistic personal privacy workflow. *Information*, *11*(7), 356.

[51] Mee, B., Kirwan, M., Clarke, N., Tanaka, A., Manaloto, L., Halpin, E., . . . , & McElvaney, N. G. (2021). What GDPR and the health research regulations (HRRs) mean for Ireland: A research perspective. *Irish Journal of Medical Science*, *190*(2), 505–514.

[52] Mocydlarz-Adamcewicz, M., Bajsztok, B., Filip, S., Petera, J., Mestan, M., & Malicki, J. (2023). Management of onsite and remote communication in oncology hospitals: Data protection in an era of rapid technological advances. *Journal of Personalized Medicine*, *13*(5), 1–13. https://doi.org/10.3390/jpm13050761

[53] Jabarulla, M. Y., & Lee, H. N. (2021). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. *Healthcare*, *9*(8), 1019.

[54] Pandit, C., Kothari, H., & Neuman, C. (2020). Privacy in time of a pandemic. In *13th CMI Conference on Cybersecurity and Privacy (CMI) – Digital Transformation – Potentials and Challenges,* 1–6. https://doi.org/10.1109/CMI51275.2020.9322737

[55] Weller, J., Boyd, M., & Cumin, D. (2014). Teams, tribes and patient safety: Overcoming barriers to effective teamwork in healthcare. *Postgraduate Medical Journal*, *90*(1061), 149–154. https://doi.org/10.1136/postgradmedj-2012-131168

[56] Minssen, T., Seitz, C., Aboy, M., & Compagnucci, M. C. (2020). The EU-US privacy shield regime for cross-border transfers of personal data under thGDPR: What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector? *European Pharmaceutical Law Review*, *4*(1), 34–50.

[57] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562.

[58] Matagi, S. O., & Kaneko, S. (2023). Challenges and opportunities on data protection and privacy in healthcare. *International Journal of Scientific Research Updates*, *5*(01), 023–041. https://doi.org/10.53430/ijsru.2023.5.1.0001

[59] Aarestrup, F. M., Albeyatti, A., Armitage, W. J., Auffray, C., Augello, L., Balling, R., . . . , & Gan, C. (2020). Towards a

European health research and innovation cloud (HRIC). *Genome Medicine*, *12*(18), 1–14. https://doi.org/10.1186/s13073-020-0713-z

[60] Dove, E. S. (2018). The EU general data protection regulation: Implications for international scientific research in the digital era. *Cambridge University Press*, *46*(4), 1013–1030. https://doi.org/10.1177/1073110518822003

[61] Dienlin, T., Masur, P. K., & Trepte, S. (2021). A longitudinal analysis of the privacy paradox. *New Media & Society*, *25*(5), 1043–1064. https://doi.org/10.1177/14614448211016316

[62] Freitas, A., Souza, J., & Caballero, I. (2023). Data governance in the health sector. In I. Caballero & M. Piattini (Eds.), *Data governance* (pp. 215–231). Springer. https://doi.org/10.1007/978-3-031-43773-1_11

[63] Jeyaraman, N., Ramasubramanian, S., Yadav, S., Balaji, S., Muthu, S., & Jeyaraman, M. (2024). Regulatory challenges and frameworks for fog computing in healthcare. *Cureus*, *16*(8), e66779. https://doi.org/10.7759/cureus.66779

[64] Udroiu, A. (2019). The GDPR training program for Romanian public institutions. In *11th International Conference on Education and New Learning Technologies*. https://doi.org/10.21125/edulearn.2019.0637

[65] March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization Science*, *2*(1), 71–87.

[66] Marelli, L., Lievevrouw, E., & Hoyweghen, I. V. (2020). Fit for purpose? The GDPR and the governance of European digital health. *Policy Studies*, *41*(5), 447–467. https://doi.org/10.1080/01442872.2020.1724929

[67] Molnár-Gábor, F., & Sellner, J. (2022). Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden. *Seminars in Cancer Biology*, *84*, 271–283. https://doi.org/10.1016/j.semcancer.2021.12.001

How to Cite: Al Khatib, I., Ahmed, N., & Ndyiaye, M. (2024). GDPR Compliance of Hospital Management Systems in the UAE. *Journal of Data Science and Intelligent Systems*. https://doi.org/10.47852/bonviewJDSIS42023640