Review Article

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2026.67.010465

Data Protection and Information Security in Prehospital Emergency Care: A Literature Review of GDPR and ISO 27001

Dimitra Pappa[1] and Emmanouil Zoulias[2]*

[1]*National Centre for Scientific Research "Demokritos", Greece*

[2]*Department of Nursing National and Kapodistrian University of Athens, Greece*

***Corresponding author:** Emmanouil Zoulias, Department of Nursing National and Kapodistrian University of Athens Greece

ARTICLE INFO

Received: October 19, 2026

Published: November 02, 2026

Citation: Dimitra Pappa and Emmanouil Zoulias. Data Protection and Information Security in Prehospital Emergency Care: A Literature Review of GDPR and ISO 27001. Biomed J Sci & Tech Res 67(2)-2026. BJSTR. MS.ID.010465.

ABSTRACT

Background: The growing digitalization of healthcare has intensified the collection, processing, storage, and transmission of sensitive patient information. The General Data Protection Regulation (GDPR) establishes a regulatory framework for personal data protection within the European Union, while ISO/IEC 27001 provides a structured framework for information security management. These requirements are particularly relevant to healthcare, where information systems process sensitive patient data.

Objective: This study aimed to examine the extent to which GDPR requirements and ISO 27001 principles have been studied and applied in prehospital emergency healthcare and to identify evidence from the broader healthcare sector that could inform their future implementation in emergency medical services.

Methods: A literature review was conducted using PubMed, Scopus, Web of Science, and Google Scholar. Searches initially combined terms for prehospital emergency care with terms for GDPR, ISO 27001, information security, and data safety. Because no studies specifically addressed prehospital emergency setting, the search was subsequently expanded to the broader healthcare domain. GDPR-related publications from 2016 onward and ISO 27001-related publications from 2005 onward were included.

Results: A total of 1,115 records were initially identified, and 53 publications were ultimately included. No publication specifically addressed data protection or ISO 27001-based information security in prehospital emergency healthcare. Of the 53 included studies, 45 concerned GDPR and healthcare, and eight concerned ISO 27001 and healthcare. The literature covered GDPR implementation in healthcare organizations, health professionals' awareness and compliance, national regulatory implementation, digital and mobile health, patient health-data sharing, electronic health records, and ISO 27001 implementation in healthcare environments.

Conclusions: A clear research gap exists regarding data protection and information security in prehospital emergency healthcare. Evidence from the wider healthcare sector underscores the importance of GDPR compliance, staff awareness, information security management, and appropriate technical and organizational safeguards. Further empirical research on ambulance services, emergency medical personnel, and prehospital health information systems is needed.

Keywords: GDPR; ISO 27001; Prehospital Emergency Care; Emergency Medical Services; Information Security; Data Protection; Health Information Systems

Abbreviations: ICT: Information and Communication Technologies; GDPR: General Data Protection Regulation; EMS: Emergency Medical Services; EHDS: European Health Data Space

Introduction

Healthcare increasingly relies on information and communication technologies (ICT) and information systems to collect, process, store, and exchange patient information. Advances in ICT have accelerated the digitization of health information, transforming how patient data are recorded, accessed, shared, and used across healthcare settings. As a result, health information systems have become an integral part of healthcare delivery, with growing emphasis on interoperability to enable the seamless exchange of information across diverse systems and settings [1]. As the volume and complexity of electronically processed health information grows, so does the importance of securing healthcare information systems [2]. Protecting this information requires a multilayered approach that addresses regulatory, organisational, and operational dimensions [3-5]. Health-related information is among the most sensitive categories of personal data. Its protection has therefore received considerable attention under the European data- protection framework, particularly Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR) [6,7]. The GDPR establishes requirements for processing personal information, strengthens data subjects' rights, and increases the accountability obligations of organizations that process personal data [6,8]. The GDPR has significant implications for healthcare, where organizations routinely collect and process sensitive patient information.

Several studies have examined its implementation in healthcare organizations and clinical settings [9,10], while others have explored patients' willingness to share personal health information under the new regulatory framework [11,12]. In 2022, the European Commission proposed the European Health Data Space (COM/2022/197), a regulatory framework intended to strengthen patients' rights over electronic health data and facilitate access to various types of data for healthcare, research, innovation, policy, regulation, and personalized medicine [13]. The proposal was subsequently adopted as Regulation (EU) 2025/327 [14], establishing a harmonized data-governance model across the European Union. The EHDS aims to give individuals greater control over and access to their electronic health records, while creating mechanisms for the secure and responsible reuse of health data for healthcare, research, innovation, and personalized medicine across the EU. A key element is the implementation of interoperable electronic health record (EHR) systems for healthcare. While the GDPR and the EHDS establish the EU-level legal and governance framework for protecting and using health data, information security is a critical operational component of data protection. Standards such as ISO/IEC 27001:2022 [15] and ISO/IEC 27701:2025 [16] provide structured frameworks for managing information security and privacy risks in support of compliance with broader European regulations. ISO/IEC 27001 sets out an approach to information security management through an Information Security Management System (ISMS), which protects the confidentiality, integrity, and availability of health records.

ISO/IEC 27701 builds on this approach by introducing a Privacy Information Management System (PIMS) to support the governance of data-subject privacy. Together, these standards complement the legal and governance requirements established by the GDPR and EHDS by offering practical frameworks for addressing information security and privacy risks. These issues are especially relevant to prehospital emergency care, where patient information is collected, accessed, and shared quickly across multiple people and locations. Prehospital emergency care includes assessing, stabilising, and treating patients, as well as transporting them to a healthcare facility [17,18]. Information and communication technologies (ICTs) support communication between ambulances and hospitals, allowing relevant patient information to reach receiving emergency departments before a patient arrives [19]. Because information is exchanged rapidly across organisational and technological boundaries, protecting patient data is particularly important in this setting. Digital technologies can improve the continuity and coordination of emergency care, but they also make it essential to protect information's confidentiality, integrity, and availability throughout its collection, processing, and transmission. Although data protection and information security have been widely examined across the healthcare sector, their implementation in prehospital emergency services remains insufficiently studied.

This review primarily examines literature on implementing the GDPR and ISO/IEC 27001:2022 in prehospital emergency healthcare settings. It also considers relevant evidence from the broader healthcare sector that may inform understanding and future implementation of information-security and data-protection practices in prehospital care. Particular attention is given to the practical application of ISO/IEC 27001 to managing information-security risks and helping organisations address applicable security requirements. However, evidence specifically addressing the application of GDPR requirements and the implementation of ISO/IEC 27001 in prehospital emergency care remains limited. Studies included in the reviewed literature have primarily examined the implementation of ISO/IEC 27001 in medical centres [20], remote patient-monitoring architectures based on Internet of Medical Things technologies [21], and other healthcare information-security settings [22,23]. Although ISO/IEC 27701:2025 provides a complementary framework for privacy management, it was not included in the review because it was published recently and relevant empirical evidence was limited at the time of the study. The EHDS Regulation (EU) 2025/327 is a recent sector-specific development, and empirical evidence on its use in prehospital emergency care remains limited. It is therefore considered part of the evolving European regulatory context rather than a primary focus of the empirical literature search.

Methods

Study Design

We conducted a structured literature review to investigate personal data protection and information system security in prehospital emergency healthcare.

The initial research questions were:

1. **Q1: To what extent are the General Data Protection Regulation and ISO 27001 applied in primary emergency prehospital healthcare?**

2. **Q2: To what extent does the existing literature address the application of the GDPR and ISO/IEC 27001:2022 to data protection and information security in prehospital emergency healthcare?**

The review focused on two complementary areas: protecting personal and health-related data under GDPR and securing healthcare information systems in relation to ISO 27001.

Information Sources and Search Strategy

We searched PubMed, Scopus, Web of Science, and Google Scholar. Additional research was performed to identify information relevant to the regulatory and organizational context. The initial search strategy combined terms such as health, prehospital, emergency, emergency care, ambulance, paramedics, and EMS (Emergency Medical Services) with GDPR, ISO 27001, information security, and data safety. Because the initial search did not identify studies specifically addressing GDPR or ISO 27001 in primary emergency prehospital healthcare, the search was broadened to the healthcare sector more generally.

For example, PubMed searches included:

(health[Title/Abstract]) AND (gdpr[Title/Abstract])

(health[Title/Abstract]) AND (iso 27001[Title/Abstract])

and

((health[Title/Abstract]) AND (gdpr[Title/Abstract])) AND (iso 27001[Title/Abstract]).

Searches by corresponding author, title, abstract, and keywords were conducted in Scopus and Web of Science.

Eligibility Criteria

The primary inclusion criterion was relevance to data protection or information security in healthcare, with particular emphasis on GDPR or ISO 27001.The initial focus was on primary emergency prehospital healthcare. However, because no publications were found in this narrowly defined setting, we also included studies from the broader healthcare environment. Studies published in English, Greek, or French were included. GDPR-related publications were considered from 2016 onward, coinciding with the adoption of Regulation (EU) 2016/679 [6]. ISO 27001-related studies were considered from 2005 onward. Both public and private healthcare organizations were eligible [24].

Study Selection

The initial search identified 1,115 records through 2023. After duplicates were removed, 523 records remained. After screening and eligibility assessment, we included 53 publications in the final synthesis. To capture more recent evidence, we conducted a targeted supplementary search for publications published after 2023. This search did not replicate the full original database search across all sources but focused on identifying recent publications relevant to the review objectives. It identified 27 studies, of which 11 met the eligibility criteria and were included in the final synthesis. These additional studies were assessed using the same inclusion criteria and incorporated to reflect recent developments in healthcare data protection, information security, and the evolving European regulatory framework. Thus, the final evidence base comprised 64 studies (Figure 1). The final evidence base included publications on GDPR implementation in healthcare organizations [9,10]; health-data privacy [25]; healthcare professionals' awareness of and guidance on GDPR [26,27]; willingness to share personal health data in connected-health environments [11,12]; digital health and GDPR compliance [28]; mobile health data protection [29,30]; privacy and security of electronic health records [31-33]; national implementation and interpretation of GDPR requirements [34-37]; and ISO 27001-related information security management and compliance in healthcare settings [20-23]. Importantly, none of the included publications specifically examined the combined issue of personal data protection and ISO 27001-based information security in primary emergency prehospital care.

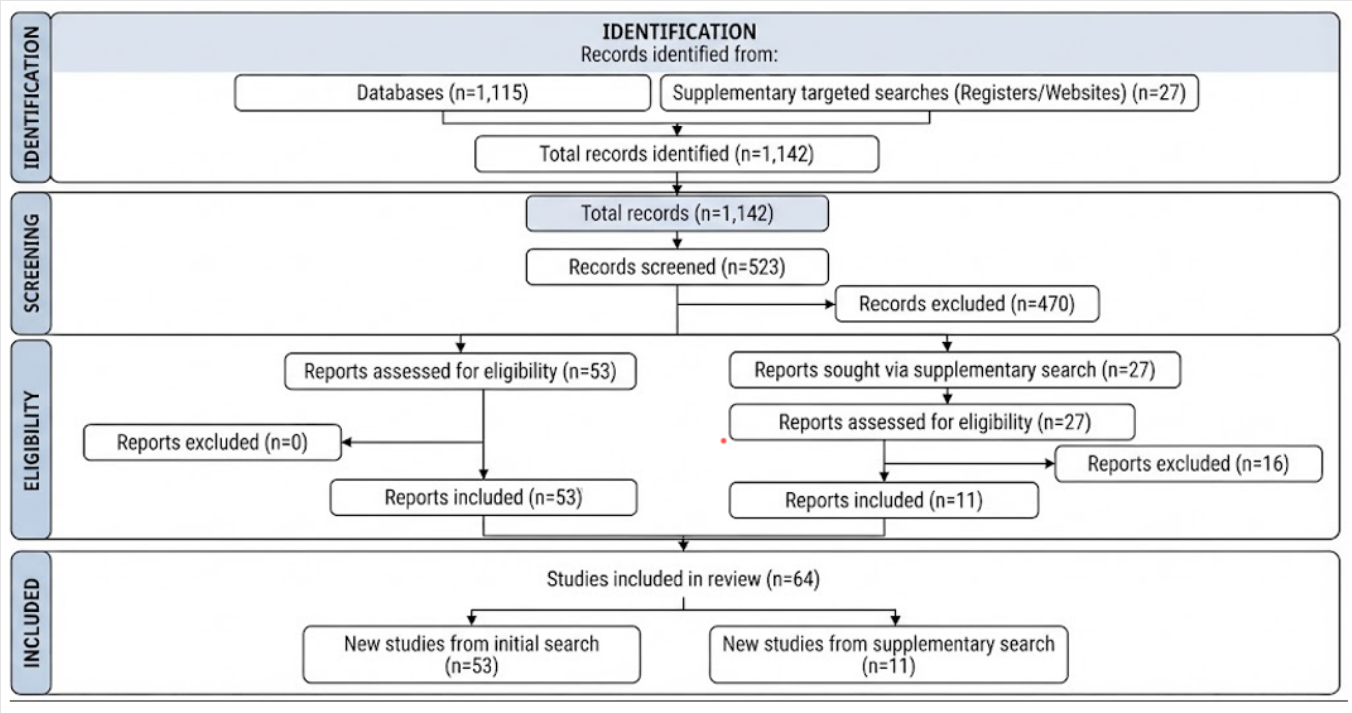


Figure 1.

Results

Study Selection and Overall Findings

The final review included 64 publications: 53 identified through the initial search and 11 through the targeted supplementary search. Of these, 54 concerned GDPR and healthcare, whereas 10 concerned ISO 27001 and healthcare. The supplementary publications broadened the evidence base by addressing recent developments in health-data governance, electronic health records, digital health, privacy-enhancing technologies, and information-security management systems. No publication specifically examined the combined application of GDPR requirements and ISO/IEC 27001-based information security management in primary prehospital emergency healthcare. Consequently, the evidence synthesis relied on research from the wider healthcare sector and should be interpreted as indirectly informing, rather than directly evaluating, prehospital practice. The included publications varied in objectives and methods. They comprised conceptual and regulatory analyses, literature reviews, qualitative and questionnaire-based studies, assessments of healthcare information systems, and studies of technologies used to process, share, or protect health information. This methodological heterogeneity precluded meaningful quantitative comparison but enabled a narrative synthesis of recurring organisational, legal, technical, and human factors relevant to healthcare data protection and information-security management.

GDPR Implementation in Healthcare

Several publications addressed the application of GDPR requirements in healthcare organisations and clinical settings. Earlier work examined GDPR compliance in health clinics [9], the protection of health-related personal data [10], and the implications of Regulation (EU) 2016/679 for health-data processing [6,7]. More recent evidence further highlights the challenges of translating regulatory requirements into operational practice. Nastasa, et al. [38] identified a regulatory gap in Romania regarding the secondary use of health data and highlighted the tension between the rapid deployment of technologies that collect, process, and store sensitive medical data and the development of adequate privacy and cybersecurity safeguards. Berzina, et al. [39] similarly addressed the practical protection of personal medical data, including organisational responsibilities, the role of the data protection officer, technical and organisational measures, informed consent, and patients' access rights. The European Health Data Space (EHDS) introduces an additional regulatory framework for health-data access and secondary use [14]. Quinn, et al. [40] examine whether the GDPR constrains EHDS health-data access bodies. As the full abstract was unavailable for verification, no more specific conclusions are attributed to that publication. Taken together, the literature suggests that implementation challenges arise not only from GDPR requirements but also from interactions between EU-level rules, national arrangements, institutional responsibilities, and mechanisms for secondary health-data use [7,14,35-37].

Knowledge and Awareness Among Healthcare Professionals

Fewer publications examined healthcare professionals' understanding and application of data-protection requirements. Markopoulou, et al. [26] investigated nursing staff awareness of personal-data processing under the GDPR, while the European Society of Radiology [27] provided professional guidance on the Regulation's implications for radiologists. Together, these publications highlight the importance of professional awareness and guidance in GDPR implementation, alongside legal, organisational, and technical safeguards [26,27]. This human dimension is particularly relevant to prehospital emergency care, where healthcare professionals must make rapid decisions about collecting, accessing, disclosing, and documenting patient information across changing locations and organisational boundaries. However, the specific implications for ambulance services apply these findings rather than examine a direct outcome in the cited publications.

National and Regulatory Implementation

Another category of publications examined GDPR implementation across national healthcare and research environments [34-37]. The literature includes work on Ireland [34], Germany, Greece, Latvia, and Sweden [35], the Netherlands [36], and Serbia [37], illustrating how a common European data-protection framework interacts with national legislation, research governance, institutional procedures, and interpretations of lawful health-data processing. More recent studies concerning Romania [38], the European Health Data Space (EHDS), and the protection of medical data further suggest that regulatory harmonisation does not automatically result in uniform operational practice. Differences in national rules, institutional capacity, technical infrastructure, and accountability arrangements may affect how health data are accessed, shared, retained, and reused. The evolving European regulatory framework, including the EHDS Regulation [14], provides additional context for these challenges.

eHealth, mHealth, and Connected Health

Much of the literature concerned digital-health environments, including eHealth, mobile health, connected health, and the secondary use of data [11,12,25,28,29,30,41]. Existing studies addressed GDPR toolkits for digital health [28], contextual approaches to mobile-health data protection [29], smartphone applications [30], and users' willingness to share personal health information [11,12]. The newer evidence extends this discussion from user attitudes to the governance and technical conditions that make data sharing acceptable. Staunton, et al. [42] note that international health-data sharing can provide important benefits but remains affected by complex rules and fragmented GDPR implementation. Their discussion of the European Health Data Space (EHDS) emphasises the need to align data governance with ethical principles and the expectations of data subjects. Flanagan and Poikela [43] examine privacy from the perspective of developers, information-security officers, and management in eHealth. Their findings underline the importance of training, documentation, organisational arrangements, regulatory clarity, and privacy-enhancing technologies. Similarly, van Drumpt, et al. [44] identify governance and permission-related gaps in implementing privacy-enhancing technologies for secondary use under the EHDS and call for further work on safe and responsible data reuse. Phuyal, et al. [45] address dynamic consent as a mechanism for managing the secondary use of health data.

This approach may give individuals more specific, informed, and revocable control over their data, but national fragmentation and limited cross-border revocation mechanisms complicate its practical operation. These findings are relevant to prehospital care because emergency information may be generated in one setting, transferred to another organisation, and later reused for care, quality improvement, research, or service planning [7,35,41].

Electronic Health Records and Cloud Environments

Several publications addressed privacy and security in electronic health records. Earlier studies evaluated openEHR against GDPR principles [31], analysed security and privacy requirements in cloud-based EHR systems [32], and considered access control in relation to explicit consent [33]. Jonnagaddala and Wong [46] extend this field to the secondary use of EHRs with large language models. Their discussion of locally deployed models, synthetic data, differential privacy, and de-identification [47] illustrates the need to adapt safeguards to new forms of data processing rather than relying exclusively on traditional access controls. Matei, et al. [48] focus on the use of emergency-department EHRs for research and quality improvement and highlight the continuing relevance of GDPR requirements and pseudonymisation when health records are reused. Although these studies do not concern ambulance services, they are relevant to the information pathway connecting prehospital teams and hospitals. They suggest that data protection should cover not only the initial collection of information but also access, transmission, linkage, secondary use, and the introduction of new analytical technologies [31,32,33].

ISO 27001 and Healthcare Information Security

A smaller but distinct body of literature addressed applying ISO/IEC 27001 in healthcare. Previous studies evaluated the standard in medical centres [20], incorporated ISO/IEC 27001 security controls into Internet of Medical Things (IoMT) architectures for remote patient monitoring [21], examined information-security and legal compliance requirements in the healthcare sector [22], and assessed knowledge and implementation of information-security management systems (ISMSs) in healthcare institutions [23]. More recent studies provide practical examples of risk-based information-security management. Basri and Ayu [49] applied ISO 31000:2018 to assess risks in a clinic information system and used ISO/IEC 27001:2022 to guide the selection of security controls. Their assessment identified 22 po-

tential risks and recommended measures such as data backups, malware protection, network security, and network segmentation. Iroth examined [50] an ISO 27001:2022-based ISMS at a BPJS Kesehatan branch and reported measures including backups, access restrictions, and password management, while identifying limited IT infrastructure and staff resistance as implementation challenges. Taken together, the literature indicates that ISO/IEC 27001 implementation involves more than formal certification. It requires systematic risk assessment, appropriate technical controls, documented procedures, staff participation, and continuing organisational support [15,20-23].

These considerations may be particularly relevant to prehospital emergency services, where information systems must operate across mobile devices, variable connectivity, organisational boundaries, and time-critical workflows. However, their applicability to prehospital settings remains an inference from the wider healthcare literature rather than a directly demonstrated finding.

Discussion

The principal finding of this review remains the absence of research specifically examining GDPR compliance and ISO/IEC 27001-based information security within prehospital emergency healthcare. The additional evidence does not alter this conclusion; rather, it clarifies the range of issues that a prehospital framework would need to address. Prehospital emergency care differs from conventional hospital care because it collects and uses information outside the healthcare facility, often under severe time pressure and with incomplete information. Ambulance personnel may access it, transmit it to a receiving emergency department, incorporate it into an EHR, and later reuse it for audit, quality improvement, research, or planning. Each transition creates potential risks involving inappropriate access, insecure transmission, uncertain responsibility, incomplete documentation, and later use beyond the original care episode [31-33]. The wider literature suggests that these risks should be addressed through complementary legal, organisational, technical, and human measures. GDPR establishes obligations concerning lawful processing, transparency, data-subject rights, accountability, and appropriate safeguards. ISO/IEC 27001 provides a structured basis for identifying information-security risks and implementing controls. Neither framework, however, can substitute for context-specific procedures that reflect ambulance workflows, mobile equipment, connectivity limitations, and the roles of emergency personnel.

Governance and Regulatory Coordination

The evidence on Romania [38], the EHDS, and cross-border health-data sharing indicates that formal harmonisation does not eliminate operational fragmentation. National rules, institutional policies, data-access bodies, and research-governance arrangements may interpret or implement common principles differently. For prehospital services, this raises questions about responsibility when information moves between ambulance providers, hospitals, regional authorities, and external technology providers. A prehospital governance model should therefore define the roles of controllers and processors, establish rules for routine and exceptional data sharing, document retention and secondary-use conditions, and specify how data-subject rights are handled when information is collected during an emergency. The unresolved interaction between GDPR and EHDS mechanisms also supports the need for clear institutional procedures rather than reliance on broad references to compliance [20-23].

Consent, Access, and Secondary Use

The literature on dynamic consent, health-data sharing, and emergency-department EHR research shows that the data lifecycle extends beyond the immediate clinical encounter. Consent and transparency may be difficult to operationalise during an emergency, while subsequent research or quality-improvement raises additional questions about legal basis, pseudonymisation, access, and revocation. Dynamic consent may be useful for later, voluntary data uses, but it cannot be assumed to solve every problem in emergency care. Prehospital systems may need separate procedures for urgent clinical processing, later patient communication, and secondary use. Access controls should follow the principle of least privilege, while pseudonymisation and de-identification should be applied where appropriate without creating a false assumption that data automatically fall outside GDPR requirements.

Human Factors and Organisational Capacity

The evidence on healthcare professionals and eHealth stakeholders highlights that compliance depends on behaviour as well as system design. Emergency personnel must be able to recognise authorised access, use secure communication channels, document disclosures, manage devices, and respond to incidents. Training should therefore be role-specific and integrated into operational procedures, not delivered only as general regulatory instruction. The implementation challenges reported in the ISO 27001 studies—particularly limited infrastructure and staff resistance—are relevant to ambulance services. A formal information-security management system may be ineffective if equipment is outdated, connectivity is unreliable, responsibilities are unclear, or staff perceive security controls as obstacles to urgent care. Implementation should therefore combine minimum technical requirements with practical workflows, leadership support, monitoring, and periodic review [6,15].

Technical Safeguards and Emerging Technologies

The EHR and digital-health literature demonstrates that the threat environment is changing. Cloud systems, connected devices, privacy-enhancing technologies, and large language models introduce new processing pathways and new possibilities for secondary use. Measures such as encryption, strong authentication, access logging, secure backups, network segmentation, pseudonymisation, de-identification, and privacy-preserving analytics should be selected through documented risk assessment [11,12,33]. The studies on pri-

vacy-enhancing technologies and LLM-related EHR use also suggest that innovation should be accompanied by governance from the design stage. In prehospital care, this principle could apply to electronic patient-care records, ambulance-to-hospital data exchange, telemedicine, automated triage support, and later analytical use of operational data. Technical safeguards should be evaluated not only for confidentiality but also for availability and integrity, since inaccessible or altered information may directly affect patient safety.

Implications for Prehospital Emergency Information Systems

The findings support examination of the complete prehospital information pathway:

Emergency call → Emergency scene → Ambulance → Data transmission → Emergency department → Hospital information system → Secondary use

For each stage, future research should assess who may access information, what data is collected, how identity and authorisation are verified, how information is transmitted and stored, how incidents are reported, and how records are retained or reused. Studies should also examine whether GDPR procedures and ISO 27001 controls remain workable during poor connectivity, device loss, multiple handovers, mass-casualty incidents, and cross-organisational care. Without direct evidence, recommendations should initially be tested through empirical case studies, usability assessments, DPIAs, and pilot implementations rather than assumed to transfer automatically from hospitals to ambulance services. A combined governance and information-security framework could then be refined around the operational realities of emergency medical services [51,52].

Data Protection Impact Assessment and Organisational Governance

DPIAs may provide a practical method for examining high-risk processing in prehospital systems, including mobile data collection, location information, image capture, cloud storage, automated decision support, and data exchange with hospitals. The data protection officer should work with information-security personnel, clinical leadership, procurement, and operational staff to assess privacy risks throughout system design and deployment [51-53]. The reviewed evidence also indicates that organisational governance should be continuous. Policies should be reviewed after incidents, system changes, new data-sharing arrangements, and the introduction of analytical tools. This is consistent with the risk-management orientation of ISO 27001 and with the GDPR principle of accountability [6,15].

Limitations

Several limitations should be considered. First, no publication specifically answered the original prehospital emergency-care research question. The scope therefore had to expand to the wider healthcare sector, and the included evidence's relevance to ambulance services is indirect. Second, the literature is heterogeneous, including regulatory analyses, reviews, questionnaire studies, technical assessments, and organisational case studies. The findings cannot therefore be interpreted as a quantitative estimate of compliance or intervention effectiveness. Third, the supplementary search was targeted rather than a complete replication of the original database search. The additional publications were included to capture recent developments, but they may not represent the entire post-2023 evidence base. Finally, not all abstracts were available in full in the reviewed material. Where only titles or limited descriptions were available, interpretation was restricted to the information that could be verified.

Conclusion

This study examined how the General Data Protection Regulation (GDPR) and information security management based on ISO/IEC 27001 are applied in primary prehospital emergency healthcare, and how existing literature has investigated these applications. Regarding the first research question (Q1), the review could not establish the extent to which the GDPR has been implemented or ISO/IEC 27001 adopted in primary prehospital emergency healthcare. While the GDPR sets requirements for protecting personal data [6] and ISO/IEC 27001 provides a structured framework for information security management [15], none of the included publications directly assessed their implementation in ambulance services or primary prehospital emergency healthcare organisations. The absence of published evidence should therefore not be taken to mean that these frameworks are not implemented in practice. For the second research question (Q2), the findings point to a substantial gap in literature. None of the 64 included publications specifically examined the combined application of GDPR requirements and ISO/IEC 27001-based information security management in primary prehospital emergency healthcare. However, research across the broader healthcare sector offers relevant evidence on GDPR implementation in healthcare organisations [9,10]; healthcare professionals' awareness and guidance [26,27]; patient attitudes towards health-data sharing [11,12]; digital and mobile health [32-35]; the privacy and security of electronic health records [36–38]; and ISO/IEC 27001 implementation in healthcare settings [20-23].

The broader evidence indicates that effective data protection and information security depend on complementary legal, organisational, technical and human measures. GDPR governance and accountability requirements [6,7], ISO/IEC 27001-based risk management [15,20-23], staff awareness [26,27], secure information exchange [19,37,38], and Data Protection Impact Assessments [40,41] can help guide the development of appropriate safeguards for prehospital information systems. However, their effectiveness and practical application in ambulance services must be established through direct empirical investigation. As digital technologies become more widely used in prehospital emergency care, sensitive patient information must be protected throughout its lifecycle: from collection at the emergency scene and

processing in the ambulance to transmission, integration into hospital information systems, and potential secondary use [19,36-38]. Future research should examine emergency medical personnel's awareness of the GDPR, information-security practices in ambulance services, secure electronic transmission of patient information, Data Protection Impact Assessments for prehospital systems [40,41], and the feasibility of implementing information-security management systems based on ISO/IEC 27001 [15,20-23]. Overall, the present study finds that the extent to which GDPR and ISO/IEC 27001 have been implemented in primary prehospital emergency healthcare remains unclear. Published research directly examining their application in this setting is extremely limited. Further empirical studies are needed to address this gap and reflect the operational, technological, and organisational characteristics of prehospital emergency care.

References

1. Haux R (2006) Health information systems—past, present, future. Int J Med Inform 75(3-4): 268-281.
2. Qureshi R, Koo I (2026) A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. Appl Sci 16(3): 1511.
3. Knezevic Ivanovski T, Honap S, Matic R, Markovic S, Peyrin-Biroulet L, et al. (2025) Building a healthcare data warehouse: considerations, opportunities, and challenges. Front Digit Health 7: 1691142.
4. Riou C, El Azzouzi M, Hespel A, Guillou E, Coatrieux G, et al. (2025) Ensuring General Data Protection Regulation compliance and security in a clinical data warehouse from a university hospital: implementation study. JMIR Med Inform 13: e63754.
5. Kruse CS, Dolezel D, Shanmugam R (2026) Cybersecurity in healthcare: a systematic review and narrative analysis. Appl Clin Inform 17(2): 315-328.
6. (2016) European Parliament, Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J Eur Union L119: 1-88.
7. Peloquin D, DiMaio M, Bierer B, Barnes M (2020) Disruptive and avoidable: GDPR challenges to secondary research uses of data. Eur J Hum Genet 28: 697-705.
8. Voigt P, von dem Bussche A (2017) The EU General Data Protection Regulation (GDPR): a practical guide. Cham: Springer International Publishing.
9. Lopes IM, Guarda T, Oliveira P (2020) General Data Protection Regulation in health clinics. J Med Syst 44(2): 53.
10. Orel A, Bernik I (2018) GDPR and health personal data; tricks and traps of compliance. Stud Health Technol Inform 255: 155-159.
11. Karampela M, Ouhbi S, Isomursu M (2019) Exploring users' willingness to share their health and personal data under the prism of the new GDPR: implications in healthcare. Annu Int Conf IEEE Eng Med Biol Soc 2019: 6509-6512.
12. Karampela M, Ouhbi S, Isomursu M (2019) Connected health user willingness to share personal health data: questionnaire study. J Med Internet Res 21(11): e14537.
13. (2022) European Commission. Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM(2022) 197 final. Strasbourg: European Commission.
14. (2025) European Parliament, Council of the European Union. Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. Off J Eur Union L 2025/327.
15. (2022) International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection—Information security management systems—Requirements. Geneva: ISO.
16. (2025) International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27701:2025. Information security, cybersecurity and privacy protection—Privacy information management systems—Requirements and guidance. Geneva: ISO.
17. Callaham M (1997) Quantifying the scanty science of prehospital emergency care. Ann Emerg Med 30(6): 785-790.
18. Ahl C, Nyström M (2012) To handle the unexpected—the meaning of caring in pre-hospital emergency care. Int Emerg Nurs 20(1): 33-41.
19. Anantharaman V, Swee Han L (2001) Hospital and emergency ambulance link: using IT to enhance emergency pre-hospital care. Int J Med Inform 61(2-3): 147-161.
20. Chang CC, Sun PR, Liao KH, Chen YF (2011) Evaluating the ISO/IEC 27001 with experts' knowledge for Taiwanese medical center. J Converg Inf Technol 6(10): 63-70.
21. Alegría B, Wong L, Bedriñana D (2022) Model for implementing a IoMT architecture with ISO/IEC 27001 security controls for remote patient monitoring. In: 2022 32nd Conference of Open Innovations Association (FRUCT).
22. Sánchez LE, Santos-Olmo A, Álvarez E, Fernández-Medina E, Mario Piattini, et al. (2012) LOPD compliance and ISO 27001 legal requirements in the health sector. IEEE Lat Am Trans 10(3): 1824-1837.
23. Rienzo A, Bustamante M, Aravena C, Lefranc G (2018) Evaluation of the degree of knowledge and implementation of information security management systems, based of the NCh-ISO 27001 standard, in health institutions. In: 2018 IEEE International Conference on Automation/XXIII Congress of the Chilean Association of Automatic Control (ICA-ACCA).
24. (2026) Information Commissioner's Office. UK GDPR guidance and resources [Internet]. Wilmslow: Information Commissioner's Office.
25. Pool J, Fatehi F, Hassandoust F, Akhlaghpour S (2020) Health data privacy: research fronts, hot topics and future directions. Stud Health Technol Inform 275: 167-171.
26. Markopoulou V, Nieri A, Liaskos J, Zoulias E, Mantas J, et al. (2020) Nursing staff's awareness of processing personal data according to GDPR. Stud Health Technol Inform 272: 237-240.
27. (2017) European Society of Radiology (ESR) The new EU General Data Protection Regulation: what the radiologist should know. Insights Imaging 8(3): 295-299.
28. Hussein R, Wurhofer D, Strumegger EM, Stainer-Hochgatterer A, Kulnik ST, et al. (2022) General Data Protection Regulation (GDPR) toolkit for digital health. Stud Health Technol Inform 290: 222-226.
29. Pool J, Akhlaghpour S, Fatehi F (2020) Towards a contextual theory of mobile health data protection (MHDP): a realist perspective. Int J Med Inform 141: 104229.
30. Laune D, Arnavielhe S, Viart F, Bedbrook A, Mercier J, et al. (2019) Règlement général sur la protection des données pour MASK-air® (application mobile rhinite et asthme). Rev Mal Respir 36(9): 1019-1031.
31. Gonçalves-Ferreira D, Sousa M, Bacelar-Silva GM, Frade S, Antunes LF, et al. (2019) OpenEHR and General Data Protection Regulation: evaluation of

principles and requirements. JMIR Med Inform 7(1): e9845.

32. Rodrigues JJPC, de la Torre I, Fernández G, López-Coronado M (2013) Analysis of the security and privacy requirements of cloud-based electronic health records systems. J Med Internet Res 15(8): e186.
33. de Carvalho Junior MA, Bandiera-Paiva P (2020) Strengthen electronic health records system (EHR-S) access-control to cope with GDPR explicit consent. J Med Syst 44(10): 172.
34. Kirwan M, Mee B, Clarke N, Aoife Tanaka, Lino Manaloto, et al. (2021) What GDPR and the Health Research Regulations (HRRs) mean for Ireland: "explicit consent"—a legal analysis. Ir J Med Sci 190: 515-521.
35. Molnár-Gábor F, Sellner J, Pagil S, Slokenberga S, Tzortzatou-Nanopoulou O, et al. (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. Semin Cancer Biol 84: 271-283.
36. Kist I (2023) Assessment of the Dutch rules on health data in the light of the GDPR. Eur J Health Law 30(3): 322-344.
37. Marovic B, Curcin V (2020) Impact of the European General Data Protection Regulation (GDPR) on health data management in a European Union candidate country: a case study of Serbia. JMIR Med Inform 8(4): e14604.
38. Nastasa I, Furtunescu FL, Minca DG (2024) Analysis of GDPR compliance in utilizing personal data for public health purposes in Romania. Maedica (Bucur) 19(2): 298-302.
39. Berzina AB, Rozsokha SS, Makhmurova-Dyshliuk OP, Pletenetska AO (2026) Protection of personal medical data in the context of GDPR implementation. Pol Merkur Lekarski 54(1): 66-72.
40. Quinn P, Ellyne E, Yao C (2024) Will the GDPR restrain health data access bodies under the European Health Data Space (EHDS)?. Comput Law Secur Rev 54: 105993.
41. Dove ES, Chen J (2020) To what extent does the EU General Data Protection Regulation (GDPR) apply to citizen scientist-led health research with mobile devices?. J Law Med Ethics 48(S1): 187-195.
42. Staunton C, Shabani M, Mascalzoni D, Mežinska S, Slokenberga S, et al. (2024) Ethical and social reflections on the proposed European Health Data Space. Eur J Hum Genet 32(5): 498-505.
43. Flanagan L, Poikela M (2025) Attitudes of developers towards privacy in personal health applications. Stud Health Technol Inform 327: 949-953.
44. van Drumpt S, Chawla K, Barbereau T, Spagnuelo D, van de Burgwal L, et al. (2025) Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies. Front Digit Health 7: 1602101.
45. Phuyal S, Bhandari M, Correia Bezerra R, Bista R, Ferreira JC, et al. (2026) Dynamic consent for secondary use of health data: challenges and opportunities under European law. JMIR Med Inform 14: e93348.
46. Jonnagaddala J, Wong ZSY (2025) Privacy preserving strategies for electronic health records in the era of large language models. NPJ Digit Med 8(1): 34.
47. Vovk O, Piho G, Ross P (2026) Evaluation of healthcare data de-identification with WiseSpace tool. Stud Health Technol Inform 336: 1793-1794.
48. Matei M, Banzi R, Rujano MA, Sergio Contrino, Giulia Irene Ghilardi, et al. (2025) Legal and ethical considerations in the use of emergency department electronic health records for research and quality improvement in emergency care: an EU project perspective. Front Disaster Emerg Med 3: 1717690.
49. Basri WS, Ayu AL (2024) Risk management in information systems: applying ISO 31000:2018 and ISO/IEC 27001:2022 controls at PMI's Central Clinic. Int J Appl Inf Manag. 4(1): 1-13.
50. Iroth RM (2025) Information security management system (ISMS) at BPJS Kesehatan Tondano: implementation of ISO 27001:2022 standard. J Jaminan Kesehatan Nasional 5(1): 62-74.
51. Dashti S, Ranise S (2020) Tool-assisted risk analysis for data protection impact assessment. In: Privacy and Identity Management: Data for Better Living: AI and Privacy. IFIP Advances in Information and Communication Technology 576: 308-324.
52. Georgiou D, Lambrinoudakis C (2021) Data protection impact assessment (DPIA) for cloud-based health organizations. Future Internet 13(3): 66.
53. Ciclosi F, Massacci F (2023) The data protection officer: a ubiquitous role that no one really knows. IEEE Secur Priv 21(1): 66-77.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2026.67.010465

Emmanouil Zoulias . Biomed J Sci & Tech Res

This work is licensed under Creative *Commons* Attribution 4.0 License

Submission Link: https://biomedres.us/submit-manuscript.php



Assets of Publishing with us

- Global archiving of articles
- Immediate, unrestricted online access
- Rigorous Peer Review Process
- Authors Retain Copyrights
- Unique DOI for all articles

https://biomedres.us/