emergency care and medicine

MDPI

Viewpoint

International Emergency Responses: Harmonizing Data Security and Protection Standards for Emergency Medical Teams

Andreas Scholtz [1], Harm-Bastian Harms [2] and Thomas Neumuth [3,*]

[1] Data Protection Unit, Universitätsklinikum Leipzig, D-04103 Leipzig, Germany; andreas.scholtz@medizin.uni-leipzig.de
[2] Johanniter-Unfall-Hilfe e.V. Competence Center European Civil Protection and Disaster Assistance (EUCC), D-60437 Frankfurt am Main, Germany; harm-bastian.harms@johanniter.de
[3] Medical School, Universität Leipzig, D-04103 Leipzig, Germany
* Correspondence: thomas.neumuth@medizin.uni-leipzig.de; Tel.: +49-341-97-12000

Abstract: Emergency medical teams (EMTs) often face complex tasks during humanitarian medical interventions. These are often accompanied by complex challenges. One such example is medical documentation and the consequent processing of secure data. The gathered data contain sensitive personal and medical information and are thus confidential. This is problematic as entities outside of the EMT unit sometimes request (parts of) these data. Such entities could be local administrative and coordinating bodies, governmental agencies, or international organizations. The mentioned data serve as the cornerstone for later decision-making processes and interventions. Furthermore, regulations are in place that govern medical procedures. However, the protocols in place for managing and protecting health data are not defined. This leaves stakeholders, such as EMTs, with inherent uncertainties about data handling. Thus, there is a need for interdisciplinary discourse to find adequate solutions. EMTs must focus on establishing robust data protection mechanisms. These need to be resilient, even under severe operational constraints. Contrary to medical care, a standardized regulatory framework for data protection is absent. This allows for the existence of key players, such as the WHO (World Health Organization) and ministries. The legal permissibility for the future use of these sensitive data remains undefined. This raises questions about balancing information for retrospective analysis and the preservation of privacy rights. This article discusses governance structures during EMT operations, which outline codes of conduct (CoC) on data security and protection. Additionally, it will make recommendations for the practical implementation of these codes. The aim is to harmonize and standardize practices across the board.

Keywords: disaster medicine; information dissemination; electronic health records; computer security; security measures

Citation: Scholtz, A.; Harms, H.-B.; Neumuth, T. International Emergency Responses: Harmonizing Data Security and Protection Standards for Emergency Medical Teams. *Emerg. Care Med.* **2024**, *1*, 193–198. https://doi.org/10.3390/ecm1020020

Academic Editor: Raimundas Lunevicius

Received: 13 March 2024
Revised: 25 May 2024
Accepted: 11 June 2024
Published: 19 June 2024

1. Introduction

Disasters at both national and international levels often surpass local response capacities. In 2010, the World Health Organization (WHO) instituted the Emergency Medical Teams (EMTs) initiative for immediate specialized healthcare support in affected areas. EMTs are predefined teams of healthcare professionals (doctors, nurses, paramedics, etc.) that treat patients affected by an emergency or disaster [1,2]. These teams are self-sufficient and can be deployed quickly. Their work involves various skills within medical, technical, and logistical fields.

Keeping medical patient records is crucial during EMT missions. This includes the handling of sensitive personal and health data. For various reasons, such data might also need to be shared with local authorities and international bodies, including patient referral, mission management, or aid coordination [3]. Safeguarding sensitive information is essential in order to prevent misuse and to uphold the quality of medical care provided.

Negligence can lead to physical, psychological, and immaterial damage for those affected. Numerous unresolved issues concerning the proper management and secure storage of data within EMT operations remain. Thus, a multi-disciplinary dialogue is imperative in order to address these challenges in an increasingly interconnected world.

While the WHO plays a pivotal role in setting global health standards, the responsibility for developing a standardized regulatory framework for data protection should be a collaborative effort involving multiple stakeholders. This includes national governments, international organizations, operators of EMTs, and members of the private sector. This ensures a comprehensive approach that reflects legal, cultural, and operational realities.

This article aims to provide insights into the data protection challenges faced by EMTs, guided by the European General Data Protection Regulation (GDPR, specifically Art. 40 GDPR 'Codes of Conduct'). The objective is to offer key considerations and foster a global discussion among stakeholders in order to develop practical solutions. These recommendations reflect the authors' interpretation of GDPR provisions relevant to EMT operations.

2. Challenges in Data Management Faced by EMTs

Emergency medical teams encounter three primary obstacles related to data management: the absence of comprehensive guidelines, heterogeneous technical–organizational systems and processes, and operations under disparate legal jurisdictions in the home country and country of deployment.

2.1. Missing Guidelines for Data Management within EMTs

Despite existing recommendations for medical procedures, e.g., [4], a lack of uniform guidelines on data management causes uncertainty among responders and related organizations, including the WHO, EMTs, national focal points (NFPs), and ministries. This extends to the lawfulness of (re)using medical data for future missions or medical research. Furthermore, patients (as the source of these medical data) have little or no control over whether or how their data are stored and might be processed in the future. Depending on the respective local or legal structure, they have limited ways of gaining control of their data. Finally, there are no standardized protocols that can be used for handling the personal data of EMT members and other parties involved. Also, during the cooperation of two or more EMTs or patient referral, discrepancies regarding technical measures of data processing occur. This is due to differing national laws on record keeping, data retention, and further processing, and it can lead to complicating legal resolutions and limit patients' control over their information.

2.2. Technical–Organizational Heterogeneity and Processes

Depending on their possibilities, EMTs document operations either electronically, using paper-based systems, or via hybrid approaches. Patient data and treatment courses are meticulously documented. Owing to the variance in medical procedures and technology, various hard- and software systems are utilized. This complicates data interoperability and the safeguarding of sensitive information during and after deployment. The absence of agreed-upon technical and organizational measures exacerbates the risks associated with data handling. This creates vulnerabilities for both EMTs and the beneficiaries of their services. Unsecured personal data could be exploited and malicious entities could sabotage EMT missions through cyberattacks [5], compromising patient treatment and mission effectiveness.

2.3. Operations under Multiple Legal Systems and Further Legal Ramifications

Further complications arise from differing national legal frameworks, exemplified by the operational experiences of European EMTs in non-European jurisdictions, such as the typhoon in the Philippines in 2013 or the Nepal earthquake in 2015. EMTs with diverse legal backgrounds might be confronted by considerable challenges when local

legal stipulations are involved, particularly concerning claims processes and the rights of affected individuals.

Regarding legal ramifications, class action lawsuits represent another significant concern. With consumer protection mechanisms being enabled in the US, class actions are now becoming increasingly important in Europe as well. They often involve financial repercussions and can be based on data infringements, such as breaches, data loss, or unauthorized tampering. Lawsuits have already been filed against various entities, such as US Radiology Specialists, Inc. [6]; Meta (Facebook); the UCSF Medical Center; and the Dignity Health Medical Foundation [7], for data breaches and the unauthorized use of medical data. Given the increasing likelihood of such actions, fueled in part by litigation financiers and legal service providers, EMTs could face substantial claims. Most notably, this holds weight if it can be proven that adequate organizational and technical safeguards were lacking.

3. Codes of Conduct as a Strategic Approach

The multifaceted landscape of international legal systems, deviating from technological infrastructures, and inconsistent data processing protocols create a challenging environment for emergency medical teams, designated as "data controllers" under Article 4, No. 7 of the General Data Protection Regulation (GDPR). To mitigate these complexities, a standardized approach for data protection and security is advisable, consolidating existing standardization in EMT medical and organizational processes. This section outlines the authors' interpretation of how EMTs can navigate these challenges by considering sector-specific codes of conduct.

Drawing upon the provisions outlined in Article 40 of the GDPR, this document analyzes the potential formulation of uniform codes of conduct (CoCs) to enhance data security and data protection measures, at least within EU member states [8]. These codes are not novel to data protection or broader regulatory compliance. They have been utilized extensively in other sectors, including global business practices. These codes are developed with a focus on sector-specific compliance and are subject to a review by supervisory authorities that seeks to ensure alignment with prevailing data protection legislation.

These CoCs serve multiple purposes: They provide organizations with a framework for action, clarify ethical and legal foundations for decision making, and foster accountability through oversight mechanisms. They also confer transparency, engendering trust among stakeholders and the broader public.

By comparison, codes of conduct for data protection specifically address the ethical and operational measures that EMTs must follow to secure their data, which are distinct from Habeas Data laws that primarily focus on the rights of individuals to access and correct their personal information.

The GDPR allows for the development of sector-specific CoCs that encapsulate both ethical and legal imperatives for adequate data protection. These codes also facilitate the convergence of other objectives, whether economic or research-driven. Standardization, therefore, is advantageous as it provides a structured transparent framework for legal and ethical data protection, particularly beneficial to member organizations.

The legislative intent behind these codes of conduct is the establishment of coherent and clear guidelines for data processing that all organizations can follow. Article 40 of the GDPR serves as a non-exhaustive guide for this operation, highlighting the core principles of data protection under Article 5 of the GDPR while leaving room for further interpretative nuances and implementation conditions raised by subsequent articles. Generally, CoCs require organizations to declare that they are subject to the self-imposed CoCs submitted by the respective industry association. Furthermore, they serve as an aid to interpretation and are committed to ensuring a monitoring body's compliance with the codes of conduct [9].

In the specific context of EMTs, emphasis is placed on ensuring effective medical care in crisis scenarios, achieving global data interoperability, and facilitating data sharing for both operational efficacy and learning. Consequently, CoCs not only offer EMT organizations

with a standardized data protection framework, but also the flexibility to tailor these guidelines according to their unique operational imperatives.

4. Principles to Comply

In compliance with Article 40 of the General Data Protection Regulation, emergency medical teams are mandated to adhere to a set of principles concerning data management, protection, and security. The objective of these principles is to align EMT practices with the stipulations provided by European legal frameworks. While most of these measures can be internally instituted by individual EMTs, certain actions—such as the formation of harmonization entities for distinct EMT codes of conduct or the inception of internationally acknowledged arbitration bodies—would benefit from a collective coordinated strategy among EMT organizations. The overall aim is to standardize, harmonize, and automate processes related to data security and protection, both in operational and research contexts.

The key areas to consider for the EMT development of data management are as follows:

- Transparent and ethical data processing: Uphold the tenets of fairness and transparency in all data-related activities.
- Legitimate interests: Ensure that data processing is indispensable and rooted in legitimate interests, particularly when viewed from an external standpoint.
- Pseudonymization: Enable further academic inquiries without jeopardizing individual privacy, as personal data should undergo pseudonymization. Traceability should be restricted to those in close professional proximity to the individual in question.
- Public disclosure: In instances of data breaches, affected individuals and the broader public must be duly informed.
- Dispute resolution: Establish a central arbitration commission to reconcile divergences arising due to multiple legal systems, thereby offering a legal safety net for both EMTs and patients.
- The protection of vulnerable groups: Exert special diligence to secure the rights of minors, their guardians, and individuals with disabilities.
- Structural safeguards: Implement ready-made technical and organizational measures to bolster data security and protection. This includes documented staff training for EMTs on the sensitivity of health data. Here, all EMTs must undergo rigorous training and achieve certification in data management and protection. This ensures that they are well equipped to handle personal and medical information responsibly and in compliance with both local and international data protection regulations.
- Incident reporting: Oblige with the prompt disclosure of any data breaches to the affected parties and, if necessary, to the public.
- International data transfers: Formulate protocols for the secure exchange of data across national borders and among international organizations, including the transmission of medical information back to the EMTs' country of origin. Furthermore, the need for interoperable platforms across different countries is fundamental for the seamless operation of EMTs. Such platforms facilitate efficient data exchange and integration, enhancing the speed and efficacy of emergency medical responses across varying legal and technological environments.

5. Conclusions

The conducted analysis emphasizes the need for standardized protocols governing security and data protection within emergency medical teams. Given the World Health Organization's mandate for EMTs to maintain global self-sufficiency, the meticulous planning and standardization of all technical and organizational procedures is crucial. While uniform guidelines for medical processes have been established, equivalent frameworks for the safeguarding and management of sensitive health data remain to be formulated.

In the conceptualization phase, due diligence must be exercised in evaluating data processing methodologies and the technologies employed. Each facet of data processing

should be scrutinized, from inception to eventual decommissioning. This should also include any potential transfer of data to additional organizations or research entities. Concurrently, efforts must be devoted to navigating legal complexities and minimizing undue constraints on individual rights and freedoms.

Article 40 of the EU's GDPR presents a foundational framework for data processing, although it is not all-encompassing. In the absence of a global legal architecture, it is advisable for EMTs operating outside European jurisdictions to strictly adhere to their respective domestic regulations at the very least.

For the establishment of globally coherent regulations, the formation of an international consortium is recommended, featuring interdisciplinary experts relevant to EMT operations. Participants should include medical professionals, IT and data security experts, ethical committee members, and legal advisors. The consortium should aim to promote universally accepted standards for hardware and software capabilities devoid of product or manufacturer bias.

Existing global benchmarks, such as ISO/IEC 27001:2022 or the NIST Cybersecurity Framework, may serve as informative references in relation to security, and the Health Level Seven International (HL7) can be used as a reference for data transmission. Advanced planning should delineate technical specifications for software and hardware, ensuring a foundational level of data security. Additionally, governance structures must be established to oversee code-of-conduct compliance, alongside contingency plans for crisis scenarios, such as cyber-attacks. A culturally sensitive communication strategy for affected individuals is essential, as is the ongoing surveillance of both processes and technologies to ensure adherence to established protocols.

For sustainable enactment, continuous training in data security and protection is imperative for EMT staff. Moreover, medical and IT technologies should be standardized as much as possible, and the developed rules of conduct must be integrated into EMT certifications of the WHO. By such means, the vision for a secure, compliant, and universally accepted approach to data management within EMTs might be realized.

Author Contributions: T.N. designed the original idea, directed the project, and critically reviewed the work. H.-B.H. provided EMT domain knowledge and A.S. provided legal domain knowledge. A.S. and T.N. wrote the manuscript. All authors discussed the results and contributed to the final manuscript. The authors read and approved the final manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This study was partially funded by the European General Directorate for Civil Protection and Humanitarian Aid Operations within the European Modular Field Hospital (EUMFH) project (ECHO/SUB/2016/739964/PREP14).

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analysis, or interpretation of the data; in the writing of the manuscript; or in the decision to publish the results.

References

1. World Health Organization. Emergency Medical Teams Initiative. Available online: https://extranet.who.int/emt/content/about-us (accessed on 25 October 2023).
2. World Health Organization. *Classification, and Minimum Standards Emergency Medical Teams*; WHO: Geneva, Switzerland, 2021; ISBN 978-9-240-02933-0.
3. World Health Organization. EMT Minimum Dat Set Gateway. Available online: https://www.mdsgateway.net/ (accessed on 25 October 2023).
4. International Committee of the Red Cross. Management of Limb Injuries during Disasters and Conflicts, Published 2016. Available online: https://www.aofoundation.org/who-we-are/about-ao/disaster-response/management-of-limb-injuries (accessed on 25 October 2023).
5. Save the Children. Save the Children Statement on Blackbaud Security Breach. Available online: https://www.savethechildren.org/us/about-us/media-and-news/2020-press-releases/save-the-children-statement-on-blackbaud-security-breach (accessed on 25 October 2023).

6. Classaction.org, US Radiology Specialists Hit with Class Action over December 2021 Data Breach. Available online: https://www.classaction.org/news/us-radiology-specialists-hit-with-class-action-over-december-2021-data-breach (accessed on 25 October 2023).
7. Meta. US Hospitals Sued for Using Healthcare Data to Target Ads. Published 2022. Available online: https://www.bleepingcomputer.com/news/security/meta-us-hospitals-sued-for-using-healthcare-data-to-target-ads/ (accessed on 25 October 2023).
8. European Data Protection Board. Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. Published online 2019. Available online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en (accessed on 25 October 2023).
9. Gola, P.; Heckmann, D. *General Data Protection Regulation, Federal Data Protection Act: DS-GVO/BDSG*, 3rd ed.; Ch. Beck: Munich, Germany, 2022; ISBN 978-3-406-78266-4.