CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 32. Núm. Ordinario (2026), pp. 130-154
·ISSN 2340-860X - ·ISSNe 2386-5229

Forensic infrastructure for investigating medical crimes in the digital era

Constantin Pisarenco[1,*]
Free International University of Moldova
Serghei Pisarenco[2]
Chiril Draganiuc Institute of Pneumology

Abstract: Healthcare digitalization has reshaped the evidentiary landscape of investigations into harmful medical incidents with potential criminal-law relevance. Electronic health records, medication administration systems, laboratory and radiology platforms, and telemedicine tools record not only clinical information but also metadata, including user actions, timestamps, version histories, and intersystem transactions. Taken together, these layers create a complex digital trace whose evidentiary value depends not only on content, but also on provenance,

[1] Ph.D. in Law, Associate Professor, Department of Law, Free International University of Moldova (ULIM), Chisinau. ORCID: https://orcid.org/0000-0001-5548-4653; E-mail: constantin.pisarenco@gmail.com (corresponding author).
[2] Doctor Habilitat of Medicine, Associate Professor. Scientific laboratory for Non-Specific Lung Diseases. ORCID: https://orcid.org/0000-0002-0638-6050; E-mail: serghei.pisarenco@gmail.com

integrity, completeness, lawfulness of acquisition, and a verifiable chain of custody. This article develops a conceptual and doctrinal-comparative framework for analysing the use of electronic medical data in criminal proceedings. The study does not rely on a structured empirical dataset or statistical testing; instead, it draws on a comparative analysis of seven jurisdictions—France, Germany, the United Kingdom, the United States, Romania, Moldova, and Ukraine—alongside the case law of the European Court of Human Rights, digital forensics standards, and the regulatory framework of digital health. The article proposes a four-level model of forensic infrastructure—digital, procedural, expert, and judicial—and introduces a heuristic functional test of investigative readiness based on independence, sufficiency, timeliness, and reproducibility. It argues that electronic medical data can function as reliable evidence only where institutional mechanisms ensure traceable origin, timely preservation, sufficiently complete extraction, and reproducible expert analysis.

Keywords: Audit Logs, Criminal Investigation, Digital Evidence, Electronic Health Records, Forensic Infrastructure, Forensic Readiness, Medical Crimes

Resumen: La digitalización de la atención sanitaria ha reconfigurado el panorama probatorio de las investigaciones sobre incidentes médicos dañosos con posible relevancia penal. Las historias clínicas electrónicas, los sistemas de administración de medicamentos, las plataformas de laboratorio y radiología y las herramientas de telemedicina registran no solo información clínica, sino también metadatos, incluidas las acciones de los usuarios, las marcas temporales, los historiales de versiones y las transacciones entre sistemas. En conjunto, estas capas conforman una huella digital compleja cuyo valor probatorio depende no solo del contenido, sino también de la procedencia, la integridad, la exhaustividad, la licitud de obtención y una cadena de custodia verificable. Este artículo desarrolla un marco conceptual y doctrinal-comparado para analizar el uso de datos médicos electrónicos en el proceso penal. El estudio no se apoya en un conjunto empírico estructurado de casos ni en pruebas estadísticas; por el contrario, se basa en un análisis comparado de siete jurisdicciones —Francia, Alemania, Reino Unido, Estados Unidos, Rumanía, Moldova y Ucrania—, junto con la jurisprudencia del Tribunal Europeo de Derechos Humanos, los estándares de informática forense digital y el marco regulatorio de la salud digital. El artículo propone un modelo de cuatro niveles de infraestructura forense —digital, procesal, pericial y judicial— e introduce una prueba funcional heurística de preparación para la investigación basada en independencia, suficiencia, oportunidad y reproducibilidad. La tesis central es que los datos médicos electrónicos solo pueden operar como prueba fiable cuando existen mecanismos institucionales que garanticen la trazabilidad de su origen, su preservación oportuna, la extracción suficientemente completa y la reproducibilidad del análisis pericial.

Palabras clave: Delitos Médicos, Evidencia Digital, Historias Clínicas Electrónicas, Infraestructura Forense, Investigación Penal, Preparación Forense, Registros De Auditoría

1. Introduction

Investigating medical cases of injury with criminal implications is one of the most challenging tasks in criminal justice. Such cases require reconstructing a clinically complex event, assessing causality under uncertainty, and distinguishing between an adverse outcome, professional error, and conduct that reaches the

threshold of criminal liability.[3,4]

For a long time, the evidence base for such proceedings consisted of paper medical records, witness statements, and forensic reports. Digitalization has transformed this environment. Electronic health records (EHRs), computerized provider order entry (CPOE) systems, electronic medication administration record (eMAR) systems, laboratory and radiology systems, and telemedicine platforms record not only clinical decisions but also the process of their formation, transmission, modification, and access.[5,6]

This change is fundamental because electronic medical data contains at least two levels of evidentiary information. The first is the visible clinical level: diagnoses, prescriptions, test results, observation records, and treatment plans. The second is the technical level: timestamps, user identifiers, audit logs, version history, access records, and intersystem exchange data.

The combination of these layers forms a multi-layered digital trace that allows for a more accurate reconstruction of the chronology and distribution of responsibility compared to traditional paper documentation.

At the same time, digital traces have a high evidentiary vulnerability. Records can be modified retrospectively, exported without metadata, transformed during migration between systems, or selectively disclosed by a healthcare organization whose actions are subject to review. Under these circumstances, the central question becomes not only the content of the record, but also the ability to prove its completeness, authenticity, and independent verifiability.[7,8]

The procedural dimension is no less important. The European Court of Human Rights has repeatedly stated that in cases of death or serious injury in the medical field, states are obliged to provide an effective mechanism for establishing the facts and, where appropriate, for prosecuting. The Court does not require that every case of medical negligence be criminalized, but it does require an investigation that is independent, adequate, and prompt. This approach has been further developed in subsequent practice.[9,10,11]

---

[3] KOHN L. T.; CORRIGAN J. M.; DONALDSON M. S. (eds.). "To Err Is Human: Building a Safer Health System", Washington, DC: National Academies Press, 2000. https://doi.org/10.17226/9728

[4] MERRY A. F.; BROOKBANKS W. "The Place of the Criminal Law in Healthcare", in: MERRY A. F.; MCCALL SMITH A. (eds.), Errors, Medicine and the Law, 2nd ed., Cambridge: CUP, 2017, pp. 310–345. https://doi.org/10.1017/9781316848050.011

[5] BOWMAN S. "Impact of electronic health record systems on information integrity: quality and safety implications", Perspectives in Health Information Management, 2013, vol. 10 (Fall), 1c. Available at: https://pubmed.ncbi.nlm.nih.gov/24159271/ (accessed on 12 January 2026).

[6] RULE A., KANNAMPALLIL T., HRIBAR M. R., DZIORNY A. C., THOMBLEY R., APATHY N. C., ADLER-MILSTEIN J. "Guidance for reporting analyses of metadata on electronic health record use", Journal of the American Medical Informatics Association, 2024, vol. 31(3), pp. 784–789. https://doi.org/10.1093/jamia/ocad254

[7] CASEY E. "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet", 3rd ed., Waltham, MA: Academic Press, 2011. Available at: https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf (accessed on 12 January 2026).

[8] CASEY E., BARNUM S., GRIFFITH R., SNYDER J., VAN BEEK H., NELSON A. "Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language", Digital Investigation, 2017, vol. 22, pp. 14–45. https://doi.org/10.1016/j.diin.2017.08.002

[9] EUROPEAN COURT OF HUMAN RIGHTS. Case of Calvelli and and Ciglio v. Italy, no. 32967/96. 2002. Available at: https://hudoc.echr.coe.int/eng?i=001-60329 (accessed on 12 January 2026).

[10] EUROPEAN COURT OF HUMAN RIGHTS. Case of Šilih v. Slovenia, no. 71463/01. 2009. Available at: https://hudoc.echr.coe.int/fre?i=001-92142 (accessed on 12 January 2026).

In the digital environment, meeting these requirements increasingly depends on the timely preservation and lawful independent retrieval of electronic medical data.

The existing scientific literature on this topic is significant but fragmented. One line of research focuses on medical law and patient safety, another on the integrity of electronic medical data and audit trail analysis, a third on procedural obligations arising from Article 2 of the Convention, and a fourth on digital forensics and procedures for handling electronic evidence.

The scientific literature on this issue is significant but fragmented, with separate research developing on patient safety, medical law, the integrity of electronic medical records, audit trails, digital forensics, and procedural safeguards for effective investigation.[12,13]

In this article, the term medical crimes is used as an analytical rather than a strictly doctrinal category. It refers to a narrow range of medical incidents in which conduct may result in criminal liability due to gross misconduct, falsification or concealment of data, or other actions that impede the establishment of factual circumstances. Additionally, the following working concepts are used: controlled evidence - data under the control of a potentially audited organization; digital trace structure - a multi-layered structure of a digital footprint; forensic readiness - the ability of an information environment to generate, store, and provide data in a form suitable for evidentiary use.

Based on this, the article pursues two objectives. First, to develop a conceptual model of a forensic infrastructure for investigating medical crimes in a digital environment. Second, to propose a functional test of investigation readiness based on the criteria of independence, sufficiency, timeliness, and reproducibility. The central hypothesis is that the evidentiary value of electronic medical data is determined not only by their content, but also by the institutional and technical conditions of their formation, storage, retrieval, analysis and evaluation.

2. Methodology

2.1. Research design and analytical approach

This study utilizes a qualitative, doctrinal, comparative design and does not rely on structured empirical data or statistical testing. Its objective is analytical and interpretive in nature, exploring how legal norms, institutional mechanisms, and technical characteristics of healthcare information systems shape the conditions for the use of electronic medical data in criminal proceedings.

The primary method is comparative legal analysis. This method is used to examine access procedures to medical data, the specifics of handling digital evidence, the role of expert institutions, and court approaches to assessing the reliability and admissibility of evidence. A doctrinal analysis of legislation, judicial practice, professional standards, and scientific literature is combined with a functional analysis of investigative capabilities. The result is an interpretive framework that explains how evidentiary reliability arises as a result of institutional organization, rather than a single procedural action.

---

[11] EUROPEAN COURT OF HUMAN RIGHTS. Case of Lopes de Sousa Fernandes v. Portugal, no. 56080/13. 2017. Available at: https://hudoc.echr.coe.int/eng?i=001-179556 (accessed on 12 January 2026).

[12] WORLD HEALTH ORGANIZATION. Global Patient Safety Action Plan 2021–2030: Towards Eliminating Avoidable Harm in Health Care. Geneva: WHO, 2021. Available at: https://iris.who.int/handle/10665/343477 (accessed on 12 January 2026).

[13] RULE A., KANNAMPALLIL T., HRIBAR M. R., DZIORNY A. C., THOMBLEY R., APATHY N. C., ADLER-MILSTEIN J. Guidance for reporting analyses of metadata on electronic health record use. 2024. Ibid.

2.2. Selection of jurisdictions and sources

The comparative analysis covers France, Germany, the United Kingdom, the United States, Romania, the Republic of Moldova, and Ukraine. These jurisdictions were selected based on differences in legal models and procedural approaches, the level of digitalization in healthcare, and the availability of regulatory and institutional sources governing the investigation of medical incidents and the use of electronic medical data. The source base includes legislation and regulations governing criminal proceedings, personal data protection and the functioning of healthcare systems, as well as institutional documents of healthcare and supervisory authorities, international standards, scientific publications in the field of medical informatics and digital forensics and the practice of the European Court of Human Rights.

The analysis for each jurisdiction is based on a comparable set of sources, including criminal procedure law, healthcare and data protection regulations, and documents regulating the organization and digital infrastructure of healthcare activities. Where available, court decisions, official reports, and other publicly available materials reflecting the practical application of relevant regulations were taken into account. The lack of regulation of certain elements of the digital evidence environment, including independent extraction of metadata, audit trails and change history, was not seen as a limitation of the study, but as a significant finding of the comparative analysis.

2.3. Analytical framework and evaluation criteria

The analysis is based on a unified analytical matrix, which includes four interrelated elements: digital infrastructure, procedural mechanisms, expert organization and judicial assessment. The digital infrastructure encompasses the architecture of medical information systems, logging, data storage, versioning, interoperability, and data export. Procedural mechanisms include legal procedures for preserving, seizing, copying, and recording digital objects. The expert component reflects the interaction of forensic science and digital forensics. The judicial level concerns criteria for assessing the origin, integrity, completeness, and verifiability of data.

Four criteria are used for the functional comparison of jurisdictions: independence, sufficiency, timeliness, and reproducibility. These criteria align with key tenets of digital evidence theory, according to which evidentiary value is determined not only by the content but also by the conditions under which the data is generated and processed.

The study was conducted in stages: first, a corpus of sources was compiled, then it was structured according to an analytical matrix, followed by an assessment based on functional criteria and the formulation of comparative conclusions. Generalizations were permitted only with regulatory and institutional support, which reduces the risk of overinterpretations.

2.4. Conceptual modelling and functional test

In addition to comparative analysis, the study uses a conceptual modeling approach. A four-level model of forensic infrastructure—digital, procedural, expert, and judicial—is applied as an analytical tool for understanding evidentiary reliability as a systemic property. This model is not a normative framework, but rather a conceptual reconstruction of the conditions under which electronic medical data may acquire evidentiary value in criminal proceedings. On this basis, a functional investigative readiness test is formulated as an analytical tool designed to identify institutional constraints and conduct a structured comparison. Its purpose is not to provide quantitative measurement, but to diagnose the conditions of evidentiary

suitability; accordingly, it is not intended to be used as a means of ranking legal systems.

The comparative analysis was conducted in four stages. In the first stage, a database of regulatory and institutional sources was compiled for each jurisdiction. In the second stage, the materials were organized into an analytical matrix. In the third stage, an assessment was conducted based on four criteria. In the fourth stage, comparative conclusions were drawn based on regulatory and institutional support. This procedure is aimed at reducing the risk of overgeneralization and increasing the verifiability of the results.

3. Results

This section presents analytical findings based on doctrinal and comparative legal materials. Its purpose is to identify institutional patterns and evidentiary risks through structured comparison and conceptual interpretation.

3.1. Medical crimes as an analytical category and the subject of forensic analysis

In comparative legal analysis, it is appropriate to consider "medical crimes" not as a unified legal term, but as a research construct. This is a provisional analytical framework that allows for the unification of diverse acts in the healthcare sector that, under certain conditions, may result in criminal liability.[14] This approach shifts the focus from the formal differences between national legal systems to the essential characteristics of behavior—the degree of public danger, the nature of the violations, and the criteria for transition from a professional error or civil tort to a criminal-law assessment.

In most legal systems, an adverse medical outcome does not in itself constitute a crime. A significant portion of incidents are settled through civil liability, disciplinary procedures, administrative oversight, and patient safety mechanisms. Criminal law intervention is subsidiary in nature and is applied only when a certain threshold of public danger is reached—for example, in cases of gross negligence, unlawful inaction, falsification or concealment of medical records, and other actions that impede the establishment of factual circumstances.

This approach is particularly important in the context of the digitalization of healthcare. While the content of medical records was the key object of analysis in paper-based systems, the research field expands significantly in the digital environment. Not only the records themselves, but also the parameters of their formation—time stamps, the sequence of user actions, change history, and intersystem transactions that can determine the reconstruction of events—are acquiring significant evidentiary value.[15,16]

As a result, forensic analysis extends beyond the interpretation of clinical content to include examination of the entire documentation infrastructure. The objects of analysis include human-readable records, metadata, audit logs, document versions, intersystem exchanges, and administrative operations affecting access, modification, deletion, and export of information. Thus, in the digital age, medical crime investigations are aimed not only at establishing the clinical

[14] MERRY A. F.; BROOKBANKS W. The Place of the Criminal Law in Healthcare. 2017. Ibid.
[15] RULE A.; CHIANG M. F.; HRIBAR M. R. "Using electronic health record audit logs to study clinical activity: a systematic review of aims, measures, and methods", Journal of the American Medical Informatics Association, 2020, vol. 27(3), pp. 480–490. https://doi.org/10.1093/jamia/ocz196
[16] RULE A., KANNAMPALLIL T., HRIBAR M. R., DZIORNY A. C., THOMBLEY R., APATHY N. C., ADLER-MILSTEIN J. Guidance for reporting analyses of metadata on electronic health record use. 2024. Ibid.

circumstances but also at analyzing the information process within which the event is recorded and subsequently reconstructed. It is within this dual—clinical and informational—perspective that the modern subject of forensic investigation is formed.

3.2. Supranational standards: Effective investigation and lawful handling of medical data

Supranational standards play a key role in assessing investigations into medical incidents with criminal implications. The European Court of Human Rights has established that Article 2 of the Convention does not require automatic criminalization of every instance of medical error, but does require the existence of an effective legal mechanism capable of establishing the factual circumstances and, if necessary, ensuring accountability.[17,18,19,20,21]

Of particular importance is the procedural aspect of Article 2. The case of Šilih v. Slovenia emphasizes the autonomous nature of the State's obligation to conduct an effective investigation, even in the absence of a found substantive violation. This means that not only the outcome but also the organization of the investigation itself must be assessed.

The decision in the case Lopes de Sousa Fernandes v. Portugal develops this approach, linking the requirements of Article 2 to the State's institutional capacity to respond to cases of serious injury. In subsequent case law, the Court analyzes the timeliness of obtaining medical documents, the independence of expert examinations, and the participation of interested parties. In the context of digitalization, compliance with these requirements is directly related to operations with electronic data. Delays in receiving audit logs may result in their loss due to automatic deletion. Formally legal disclosure of information may be insufficient if the data is generated by the healthcare organization itself and is not independently verifiable.

The second important aspect concerns the lawfulness of processing medical data. Medical information is classified as data with a high level of protection, which requires a legal basis for access, adherence to the principle of proportionality, and traceability of data processing.[22,23,24] Thus, effective investigation in the digital

---

[17] EUROPEAN COURT OF HUMAN RIGHTS. Case of calvelli and Ciglio v. Italy, no. 32967/96. 2002. Ibid.

[18] EUROPEAN COURT OF HUMAN RIGHTS. Case of Šilih v. Slovenia, no. 71463/01. 2009. Ibid.

[19] EUROPEAN COURT OF HUMAN RIGHTS. Cauza Eugenia Lazăr v. Romania, no. 32146/05, 2010. Available at: https://hudoc.echr.coe.int/eng?i=001-123214 (accessed on 12 January 2026).

[20] EUROPEAN COURT OF HUMAN RIGHTS. Case of Arskaya v. Ukraine, no. 45076/05, 2013. Available at: https://hudoc.echr.coe.int/eng?i=001-138590 (accessed on 12 January 2026).

[21] EUROPEAN COURT OF HUMAN RIGHTS. Case of Tretyakova v. Ukraine, no. 63126/13, 2021. Available at: https://hudoc.echr.coe.int/eng?i=001-212963 (accessed on 12 January 2026).

[22] EUROPEAN UNION. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance). Official Journal of the European Union, 2025. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0327 (accessed on 12 January 2026).

[23] UNITED KINGDOM. Data Protection Act 2018. London: legislation.gov.uk, current version. Available at: https://www.legislation.gov.uk/ukpga/2018/12 (accessed on 12 January 2026).

[24] REPUBLIC OF MOLDOVA. Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Chișinău: Legis.md, current version. Available at: https://www.legis.md/cautare/getResults?doc_id=148996&lang=ro# (accessed on 12 January 2026). At the date of this study, Law No. 133/2011 remained applicable in the Republic of Moldova; however, it was scheduled to be repealed and replaced by Law No. 195/2024 on 23 August 2026.

environment requires the simultaneous fulfillment of two requirements: establishing the factual circumstances and lawful handling of sensitive data.

3.3. Electronic medical data as evidence: Digital trace structure and principal risks

Electronic medical data typically does not represent a single evidentiary entity. In a typical clinical process, relevant information is distributed across multiple subsystems. An electronic medical record may contain notes and prescriptions, a medication administration system may contain administration records, laboratory and radiology systems may contain raw results and timestamps, and an integration layer records the transfer of data between systems. As a result, a legally significant event is distributed across various technological layers.

From an architectural perspective, such systems typically have a multi-tiered structure, including: (1) a clinical data entry and recording layer (EHR, CPOE, eMAR), (2) transactional databases, (3) logging subsystems (audit logs), and (4) data exchange integration interfaces (e.g., HL7 or FHIR). Audit logs can be generated at the application (user actions), database (record modification operations), or system infrastructure (authentication and access) levels, with each of these levels having varying evidentiary value.

From an evidentiary analysis perspective, data provenance, integrity, completeness, and attribution are of fundamental importance. Audit logs typically contain at least the user ID, timestamp, action type (create, modify, view, delete), object ID, and system context.[25,26] However, their evidentiary value is significantly reduced in the absence of time synchronization between subsystems, limited storage periods, lack of record versions registration, or the inability to extract a complete change history.[27,28]

Research shows that audit logs can significantly enhance the analysis of clinical activity, allowing for the reconstruction of the sequence of actions and the identification of discrepancies between the content of the record and the actual course of events. However, the availability of digital data does not guarantee its evidentiary validity. Given cyber risks and the heterogeneity of information systems, the lack of adequate data storage and verification procedures complicates the assessment of its reliability.[29,30]

The issue of interoperability is particularly important. While the use of data exchange standards (such as HL7 and FHIR) facilitates system interaction, data transfer can lead to record structure transformations and loss of some metadata,

---

[25] ISO/IEC. ISO/IEC 27037:2012 – Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: International Organization for Standardization, 2012. Available at: https://www.iso.org/standard/44381.html (accessed on 12 January 2026).

[26] D'ANNA T., PUNTARELLO M., CANNELLA G., SCALZO G., BUSCEMI R., ZERBO S., ARGO A. "The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data", Healthcare, 2023, vol. 11(5), p. 634. https://doi.org/10.3390/healthcare11050634

[27] RULE A.; CHIANG M. F.; HRIBAR M. R. Using electronic health record audit logs to study clinical activity: a systematic review of aims, measures, and methods. 2020. Ibid.

[28] RULE A., KANNAMPALLIL T., HRIBAR M. R., DZIORNY A. C., THOMBLEY R., APATHY N. C., ADLER-MILSTEIN J. Guidance for reporting analyses of metadata on electronic health record use. 2024. Ibid.

[29] AL MAMUN, A.; AZAM, S.; GRITTI, C. "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction", IEEE Access, vol. 10, 2022, p. 5768–5789. https://doi.org/10.1109/ACCESS.2022.3141079

[30] WASSERMAN L.; WASSERMAN Y. "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)", Frontiers in Digital Health, 2022, vol. 4, 862221. https://doi.org/10.3389/fdgth.2022.862221

which directly impacts the completeness of the evidence base.[31]

Key architectural risks include: log overwriting due to limited retention periods, lack of time synchronization, inability to extract change history, and dependence on system vendors for data export. Taken together, these factors can lead to a situation in which a verifiable digital asset is missing by the time an investigation begins. Thus, electronic medical data should be considered as a multilayered digital trace, the evidentiary value of which is determined not only by the content, but also by the architecture of the information system and the conditions for the formation, storage and retrieval of data.

3.4. Comparative institutional models of medical-incident investigation

A comparative analysis reveals recurring institutional configurations within which medical incidents are documented, verified, and subsequently transformed into evidence. The characteristics presented are analytical and interpretive in nature and are based on normative, institutional, and scientific sources; they are not based on a structured empirical case file or a quantitative assessment of legal systems.

The jurisdictions under consideration demonstrate not so much unique models as variations of several typical approaches.

France exemplifies a multi-layered institutional configuration in which mechanisms for compensation and analysis of medical incidents coexist with criminal proceedings. This structure is reflected, in particular, in the provisions of the Code de la Santé Publique, which regulate access to medical information, as well as the Code de Procédure Pénale, which defines procedural mechanisms for investigation.

The functioning of the medical incident compensation system, including the activities of Office national d'indemnification des accidents médicaux (ONIAM), facilitates earlier recording of adverse outcomes. However, this institutional architecture alone does not guarantee the extraction of digital data at a level that allows for independent verification, particularly with regard to metadata and audit logs.

Germany is characterized by a procedurally oriented model with a developed forensic medical system. The corresponding institutional framework is formed, in particular, by the provisions of the Strafprozessordnung (Criminal Procedure Code), as well as civil law provisions, including §§ 630f-630g BGB, which establishes requirements for medical documentation.

However, available regulatory and institutional materials suggest that digital metadata extraction and standardization procedures are not always formalized as an independent element of the evidentiary process. As a result, the system's high expert capacity may be combined with a dependence on technically incomplete data sets provided by medical organizations.

The United Kingdom represents a different institutional configuration, in which independent patient safety investigation mechanisms play a significant role. These mechanisms are implemented, in particular, through the activities of the Health Services Safety Investigations Body (HSSIB), as well as through NHS England regulations, including the Records Management Code of Practice 2021.

These mechanisms are aimed at identifying the systemic causes of errors and preventing their recurrence. However, the materials obtained through these procedures are not always transformed into a form suitable for use in criminal proceedings. This creates an institutional gap between the independence of the

[31] TABARI, P.; COSTAGLIOLA, G.; DE ROSA, M.; BOEKER, M. "State-of-the-Art Fast Healthcare Interoperability Resources (FHIR)–Based Data Model and Structure Implementations: Systematic Scoping Review", JMIR Medical Informatics, vol. 12, 2024, e58445. https://doi.org/10.2196/58445

investigation and the requirements of evidence reproducibility, including the chain of custody.

The United States exhibits a combination of a high degree of digitalization and institutional fragmentation of the healthcare system and information system providers. Data access is regulated, in particular, by HIPAA regulations, including provisions for disclosure for law enforcement purposes. Despite the presence of formal access mechanisms, the actual quality of the data obtained can vary significantly depending on the specific institutional and technical environment. Thus, a high level of digital maturity does not preclude variability in the evidentiary suitability of data due to differences in logging practices, storage, and system interoperability.

This is supported by studies of interoperability and exchange of medical data, which show significant variation in practices between institutions.

Romania, the Republic of Moldova, and Ukraine demonstrate an institutional configuration in which criminal procedure mechanisms and forensic medicine retain a central role, while digital infrastructure and independent data extracting procedures are unevenly developed. In Romania, legal regulation is based on the Criminal Procedure Code and the Health Care Reform Law; in the Republic of Moldova, on the Criminal Procedure Code and the Health Protection Law; in Ukraine, on the Criminal Procedure Code and regulations governing the electronic health system, including Ministry of Health Order No. 587/2020.

In these jurisdictions, access to data in practice often depends on the technical capacity and organizational support of healthcare institutions, which increases the risk of building an evidence base based on controlled sources and limits the ability to independently verify digital data.

The practical implications of these issues are particularly evident in legal systems where the determination of liability for medical incidents depends to a large extent on expert assessment and the availability of reliable digital evidence.

A good example is Croatia, where medical malpractice ("unsuccessful medical treatment") is recognized as a separate criminal offence. In most continental legal systems, however, such acts are instead dealt with under general provisions concerning negligence or the improper performance of professional duties. This approach aims to achieve better protection of patients' rights through enhancement of criminal law.

At the same time, establishing criminal liability in such cases largely depends on the results of forensic medical examinations, which make it possible to determine the existence of a cause-and-effect connection between the actions of the healthcare professional and the resulting consequences. In this regard, the quality, objectivity and independence of the expert examination, including the analysis of electronic medical records, audit logs and other digital data, are of particular importance.[32]

A comparative analysis shows that the evidentiary validity of electronic medical data is determined not by individual system elements, but by the degree of their consistency. A strong expert base does not compensate for the shortcomings of digital infrastructure, and a high level of digitalization does not eliminate problems of procedural independence. The coordinated functioning of information system architecture, legal access mechanisms, expert competence, and judicial evaluation criteria is crucial. It is additionally noted that even with a high degree of digitalization, risks associated with the heterogeneity of system architecture and differences in data logging and storage mechanisms remain. Additionally, research

[32] VULETIĆ, I. "Medical Malpractice as a Separate Criminal Offense: A Higher Degree of Patient Protection or Merely a Sword Above the Doctors' Heads? The Example of the Croatian Legislative Model and the Experiences of its Implementation", Medicine, Law & Society, 12(2), 2019, pp. 39-60. https://doi.org/10.18690/10.18690/mls.12.2.39-60.2019

into healthcare cybersecurity points to systemic vulnerabilities that impact data integrity and availability. The problem of interoperability and data standardization also remains significant, despite the development of digital infrastructures.

Table 1 presents a condensed analytical matrix of the above configurations. It is descriptive and interpretive in nature and is intended to structure the comparison, not to quantify or rank legal orders.

Table 1. Comparative analytical matrix of selected jurisdictions (with embedded legal anchors).

Jurisdiction /Regulatory acts	Institutional configuration	Access to digital medical data	Expert configuration	Main evidentiary vulnerability
France[33,34,35]	Compensation and incident-review mechanisms coexist with criminal procedure	Legally available, but evidentiary transition may rely on provider-generated datasets	Commission-based review and court-appointed experts (including ONIAM framework)	Early documentation is relatively strong, but independent extraction of metadata and audit logs is limited
Germany[36,37,38,39]	Criminal-procedure-centered model with strong medico-legal institutions	Formal legal access exists, but extraction and standardization of metadata are not fully proceduralized	Strong forensic medicine and medico-legal expertise (supported by ePA infrastructure via gematik)	High expert capacity may depend on technically incomplete or provider-filtered datasets

[33] FRANCE. Code de procédure pénale. Paris: Legifrance, current version. Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154 (accessed on 12 May 2026).
[34] FRANCE. Code pénal. Paris: Legifrance, current version. Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719 (accessed on 12 May 2026).
[35] FRANCE. Code de la santé publique, art. L1111-7. Paris: Legifrance, current version. Available at: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042685313 (accessed on 12 January 2026).
[36] GERMANY. Strafprozessordnung (StPO). Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/stpo/ (accessed on 12 January 2026).
[37] GERMANY. Bürgerliches Gesetzbuch (BGB), 630f–630g. Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/bgb/index.html#BJNR001950896BJNE271701360 (accessed on 12 January 2026).
[38] GERMANY. Sozialgesetzbuch V (SGB V), 342. Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/sgb_5/index.html#BJNR024820988BJNE079305126 (accessed on 12 January 2026).
[39] GERMANY. Sozialgesetzbuch V (SGB V), 355. Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/sgb_5/index.html#BJNR024820988BJNE080606126 (accessed on 12 January 2026).

Jurisdiction /Regulatory acts	**Institutional configuration**	**Access to digital medical data**	**Expert configuration**	**Main evidentiary vulnerability**
United Kingdom[40,41,42]	Parallel structure of criminal procedure and independent patient-safety investigations	Safety investigations produce detailed data, but are not automatically convertible into criminal evidence	Independent investigations (HSSIB) combined with external expert analysis	Institutional independence does not ensure evidentiary reproducibility or chain-of-custody integrity
United States[43,44,45,46]	Digitally advanced but institutionally fragmented, combining regulatory and litigation-based access	Subpoenas and HIPAA-compliant disclosure pathways exist, but data quality varies across providers and systems	Adversarial and interdisciplinary expert environment, supported by certification standards (ONC)	High digital maturity coexists with uneven logging practices, retention policies, and interoperability
Romania[47,48,49]	Criminal-procedure-centered system in a developing digital health environment	Legal access is established, but operational extraction is often mediated by healthcare providers	Forensic medicine remains central, supported by national digital infrastructure (CNAS)	Limited standardization of audit log extraction and inconsistent data retention practices

[40] UNITED KINGDOM. Police and Criminal Evidence Act 1984. London: legislation.gov.uk, current version. Available at: https://www.legislation.gov.uk/ukpga/1984/60 (accessed on 12 January 2026).
[41] UNITED KINGDOM. Data Protection Act 2018. 2018. Ibid.
[42] UNITED KINGDOM. Health and Care Act 2022. London: legislation.gov.uk, current version. Available at: https://www.legislation.gov.uk/ukpga/2022/31 (accessed on 12 January 2026).
[43] UNITED STATES. Health Insurance Portability and Accountability Act (HIPAA), 45 CFR § 164.512(f). Washington, DC: Electronic Code of Federal Regulations, current version. Available at: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.512 (accessed on 12 January 2026).
[44] UNITED STATES. Health Insurance Portability and Accountability Act (HIPAA), 45 CFR § 164.312. Washington, DC: Electronic Code of Federal Regulations, current version. Available at: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312 (accessed on 12 January 2026).
[45] UNITED STATES. Federal Rules of Criminal Procedure, Rule 41. Washington, DC: United States Courts, current version. Available at: https://www.law.cornell.edu/rules/frcrmp/rule_41 (accessed on 12 January 2026).
[46] UNITED STATES. 21st Century Cures Act; ONC Certification Criteria (45 CFR § 170.315). Washington, DC: Office of the National Coordinator for Health Information Technology, current version. Available at: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-170/section-170.315 (accessed on 12 January 2026).
[47] ROMANIA. Codul de procedură penală (Legea nr. 135/2010). Bucharest: Portal Legislativ, current version. Available at: https://legislatie.just.ro/Public/DetaliiDocument/210279 (accessed on 12 January 2026).
[48] ROMANIA. LEGE nr. 95 din 14 aprilie 2006 privind reforma în domeniul sănătății. Bucharest: Portal Legislativ, current version. 2015. Available at: https://legislatie.just.ro/Public/DetaliiDocument/71139 (accessed on 12 January 2026).
[49] ROMANIA. LEGEA drepturilor pacientului nr. 46 din 21 ianuarie 2003. Bucharest: Portal Legislativ, current version. Available at: https://legislatie.just.ro/Public/DetaliiDocument/296139 (accessed on 12 January 2026).

Jurisdiction /Regulatory acts	Institutional configuration	Access to digital medical data	Expert configuration	Main evidentiary vulnerability
Moldova[50,51,52]	Criminal-procedure-centered model with emerging digital infrastructure	Access to data depends heavily on institutional cooperation and technical capacity	Forensic medicine remains central within a developing institutional framework (CNAM, Ministry of Health)	High dependence on provider-controlled data and incomplete availability of technical data layers
Ukraine[53,54,55]	Criminal-procedure-centered system with evolving electronic healthcare architecture	Legal framework for digital data exists, but practical access and preservation remain uneven	Forensic medicine supported by national health system institutions (NHSU)	Uneven preservation of digital traces and limited access to full metadata and audit layers

Note: The table presents an interpretative comparative matrix based on the analytical dimensions applied in this study (institutional configuration, access to digital medical data, expert structure, and evidentiary vulnerability). Legal references in parentheses indicate representative and non-exhaustive process, digital/health, and institutional anchors used to support the comparative analysis. The matrix is descriptive and analytical in nature and does not constitute a quantitative ranking or an empirical measurement of legal systems.

3.5. Forensic infrastructure: A four-level model

The concept of forensic infrastructure is used in this study as an analytical framework to explain how the evidentiary reliability of electronic medical data is formed. The underlying premise is that such reliability is determined not by the data content itself, but by the conditions under which it is generated, stored, retrieved, and evaluated. Evidentiary value arises from the interaction of technical,

[50] REPUBLIC OF MOLDOVA. Codul de procedură penală al Republicii Moldova nr. 122-XV din 14 martie 2003. Chișinău: Legis.md, current version. Available at: https://www.legis.md/cautare/getResults?doc_id=154997&lang=ro (accessed on 12 January 2026).

[51] REPUBLIC OF MOLDOVA. Legea nr. 411-XIII din 28 martie 1995 privind ocrotirii sănătății. Chișinău: Legis.md, current version. Available at: https://www.legis.md/cautare/getResults?doc_id=151100&lang=ro (accessed on 12 January 2026).

[52] REPUBLIC OF MOLDOVA. Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. 2011. Ibid.

[53] UKRAINE. The Criminal Procedural Code of Ukraine: Code of Ukraine, Law No. 4651-VI of 13 April 2012, revision of 1 August 2025. Legislation of Ukraine database / Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/4651-17 (accessed on 12 January 2026).

[54] UKRAINE. CABINET OF MINISTERS. Деякі питання електронної системи охорони здоров'я [Some Issues of the Electronic Health Care System]: Resolution No. 411 of 25 April 2018, revision of 4 February 2025. Legislation of Ukraine database / Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/411-2018-%D0%BF (accessed on 12 January 2026).

[55] UKRAINE. MINISTRY OF HEALTH. Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я [Some issues relating to the maintenance of the Register of medical records, referral records and prescriptions in the electronic healthcare system]: Order No. 587 of 28 February 2020; registered by the Ministry of Justice of Ukraine on 5 March 2020 under No. 236/34519; revision of 21 November 2025. Legislation of Ukraine database / Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/z0236-20 (accessed on 12 January 2026).

procedural, expert, and judicial factors.

In the context of digitalization of healthcare, this infrastructure can be represented as a system of four interconnected levels: digital, procedural, expert, and judicial. The proposed model is conceptual in nature and is used as an analytical tool; it does not constitute a normative framework or prescriptive standard.

The digital layer encompasses the architecture of medical information systems and the structure of the digital footprint they create. This footprint is multilayered and includes clinical records, audit logs, record origin and modification data, intersystem interactions, and infrastructure parameters.[56,57] Research shows that audit logs and metadata enable the reconstruction of clinical processes and the identification of discrepancies between the apparent content of a record and the actual sequence of actions.

From a forensic perspective, these characteristics determine whether a digital trace can be reconstructed as a reproducible sequence of events rather than as a static document. In this regard, the completeness of logging, the integrity of the original data, the ability to extract information without its transformation, and the documentability of data acquisition procedures are of fundamental importance.

The evidentiary suitability of a digital environment requires system logging, time synchronization, log integrity, access to change history, and the ability to extract data without losing its structure. However, the lack of standardized procedures for independent data extraction remains a significant limitation: in some cases, such procedures depend on the information system provider or the healthcare organization itself, which reduces the reproducibility and verifiability of the evidence base.

In the absence of the specified conditions, it becomes difficult to distinguish between the absence of an event and the absence of its recording, which directly affects the possibility of a reliable reconstruction of the circumstances of the case.

The procedural level includes the legal grounds for access to medical data, preservation mechanisms, procedures for removal, copying, and recording, as well as guarantees of independent retrieval. Digital forensics emphasizes that the timeliness and controllability of data acquisition procedures are key to their evidentiary value.[58,59]

The lack of operational storage mechanisms can lead to the loss or modification of data even before its analysis begins.

The expert level reflects the need for collaboration between forensic medicine and digital forensics. Interpretation of medical circumstances requires consideration of the conditions under which the record was created, while analysis of logs and metadata is impossible without understanding the clinical context. A key requirement is the reproducibility of expert analysis, which requires preserving the original data, documenting procedures, and making the methods used transparent.

The judicial level is concerned with assessing the admissibility and reliability of

---

[56] RULE A., KANNAMPALLIL T., HRIBAR M. R., DZIORNY A. C., THOMBLEY R., APATHY N. C., ADLER-MILSTEIN J. Guidance for reporting analyses of metadata on electronic health record use. 2024. Ibid.

[57] ISO/IEC. ISO/IEC 27037:2012 – Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012. Ibid.

[58] CASEY E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 2011. Ibid.

[59] KENT K.; CHEVALIER S.; GRANCE T.; DANG H. "Guide to Integrating Forensic Techniques into Incident Response". NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology, 2006. Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf (accessed on 12 January 2026).

electronic medical data. In a digital environment, such an assessment requires a separate analysis of the data's origin, integrity, completeness, and reproducibility. In modern digital evidence theory, these characteristics are considered constitutive elements of evidentiary value, rather than auxiliary features.

Thus, the evidentiary reliability of electronic medical data can be characterized as a systemic property. Violation of requirements at any level—digital, procedural, expert, or judicial—reduces the evidentiary value of the information and limits the ability to establish factual circumstances. In this study, this model is used as an analytical tool for identifying institutional bottlenecks, rather than as a means of quantitatively comparing systems.

3.6. Expertise circuit: Integrating forensic medicine and digital forensics

Forensic medical examination remains crucial in medical crime cases, as issues of causation, standard of care, mechanism of injury, and timing of effects require specialized medical knowledge.[60]

At the same time, the digitalization of healthcare is changing the requirements for expert analysis. It's not enough to view a clinical record as a static and self-contained entity; it's necessary to consider the conditions under which it was created and potential changes in the digital environment.

In particular, the forensic examination may include an analysis of how the recording was created, whether it was subsequently modified, whether warnings or signals were generated by the system, and whether technical features or failures could have affected the time of recording of the information or its availability to medical personnel.

Thus, the subject of expert assessment goes beyond clinical content and includes characteristics of the information system.

This doesn't mean that every case requires a full-fledged technical team. However, the investigation structure should allow for collaboration between clinical and digital forensics. A forensic scientist can assess the clinical significance of a drug administration delay, but determining whether the recording reflects the actual sequence of events or the result of subsequent editing may require analysis of audit logs and other technical data.

In the absence of such interaction, the digital environment remains opaque, which can distort both the prosecution and the defense.

A key methodological element uniting these areas is the reproducibility of expert analysis. Reproducible analysis requires preserving the original data set, documenting the procedures for obtaining it, recording technical parameters, specifying the software tools used and the sequence of analytical steps, and distinguishing between the stages of data processing and interpretation.

This is especially important in cases where statistical methods and machine learning algorithms are used, the use of which is acceptable but requires transparency and the possibility of independent verification.[61,62]

A model based on interdisciplinary collaboration appears to be the most appropriate. Forensic science is not a substitute for digital forensics, just as digital

---

[60] DETTMEYER R. B.; VERHOFF M. A.; SCHÜTZ H. F. "Forensic Medicine: Fundamentals and Perspectives". Berlin, Heidelberg: Springer, 2014. https://doi.org/10.1007/978-3-642-38818-7

[61] CHEN B., ALRIFAI W., GAO C., JONES B., NOVAK L., LORENZI N., FRANCE D., MALIN B., CHEN Y. "Mining tasks and task characteristics from electronic health record audit logs with unsupervised machine learning", Journal of the American Medical Informatics Association, 2021, vol. 28(6), pp. 1168–1177. https://doi.org/10.1093/jamia/ocaa338

[62] RULE A., KANNAMPALLIL T., HRIBAR M. R., DZIORNY A. C., THOMBLEY R., APATHY N. C., ADLER-MILSTEIN J. Guidance for reporting analyses of metadata on electronic health record use. 2024. Ibid.

forensics is not a substitute for clinical expertise. Their coordinated application allows for the transformation of electronic medical data into evidence capable of withstanding adversarial scrutiny.

3.7. Functional test of investigative readiness

To operationalize the proposed four-level model, the article applies a functional investigative readiness test. It is used as an analytical tool to structure the assessment of the evidentiary value of electronic medical data and identify institutional limitations. The test is not oriented toward quantitative measurement and does not involve statistical validation or ranking of legal systems; its purpose is to make the conditions for determining the evidentiary value of data conceptually transparent and comparable.

The test combines four interrelated questions: can the relevant data be stored and retrieved outside the effective control of the organization whose actions are being reviewed; does the evidentiary body include not only human-readable records but also the technical layers necessary to reconstruct the origin and chronology of events; is it possible to preserve the data before it is deleted, overwritten, or lost due to system features; can the expert analysis be independently repeated and verified.

The test thus relies on four criteria: independence, sufficiency, timeliness, and reproducibility. Each of these reflects not an abstract quality of the digital environment, but a specific condition under which electronic medical data may gain or lose evidentiary value.

Independence means the ability to store and extract data without effective control by the audited organization. If the generation of evidence is entirely dependent on the healthcare facility or system provider, the risk of selective reporting increases and the possibility of external verification is reduced.

Sufficiency requires the presence of not only visible clinical records but also metadata, audit logs, change histories, and, where necessary, information on intersystem interactions. Without these layers of digital trace, reconstructing the chronology of events and data origins remains incomplete.

Timeliness characterizes the ability to preserve data before it is deleted, overwritten, or lost due to technical features of the system or the lack of operational preservation procedures. In the digital environment, this criterion is often critical, since even a formal right of access to data does not guarantee its availability by the time an investigation begins.

Reproducibility means the ability to re-examine an expert's analysis based on a preserved source data set, documented processing procedures, and transparent analytical steps. In other words, it's not just about being able to formulate an expert's conclusion, but also about demonstrating how that conclusion was reached and enabling other experts to verify the same source data using the described procedures.[63,64]

Table 2 presents the criteria in a simplified analytical matrix. Categories 0–1–2 should be treated as conventional conceptual markers rather than as quantitative indicators or statistical values. Their function is to distinguish between typical institutional states—the absence of the relevant condition, its partial implementation, or the presence of a form that provides greater evidentiary validity of the data.

---

[63] D'ANNA T., PUNTARELLO M., CANNELLA G., SCALZO G., BUSCEMI R., ZERBO S., ARGO A. The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data. 2023. Ibid.

[64] CASEY E., BARNUM S., GRIFFITH R., SNYDER J., VAN BEEK H., NELSON A. Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. 2017. Ibid.

Table 2. Functional test of investigative readiness for electronic medical evidence.

Criterion	**Analytical question**	**0**	**1**	**2**
Independence	Can data be preserved and extracted without effective control of the investigated organization?	Extraction is fully provider-controlled	Legal access exists, but extraction remains provider-mediated	Independent extraction or auditable third-party / forensic acquisition is available
Sufficiency	Does the dataset include visible records together with metadata, logs, and version history?	Only human-readable records are available	Partial metadata or logs are available	A sufficiently complete dataset includes audit trails, version history, and relevant integration events
Timeliness	Can data be preserved before overwriting, deletion, or system loss?	No urgent preservation mechanism or unmanaged short retention	Preservation is possible but slow or uneven	Prompt preservation mechanisms and retention practices support evidentiary use
Reproducibility	Can expert analysis be independently repeated and checked?	Method is opaque and the source dataset is not preserved	Method is only partly documented	Method, source files, analytical steps, and verification trail are documented and repeatable

Note: The model is heuristic and purely analytical. The categories (0–1–2) do not represent empirical measurements, statistical scales, or validated scores. They are simplified conceptual markers used to distinguish typical institutional configurations and evidentiary conditions.

The practical significance of this test is most clearly demonstrated in a typical investigation scenario. Suppose a patient dies after a suspected delay in administering a medication. Initially, investigative authorities often receive a printout of the electronic medical record generated by the healthcare organization itself. While such a document may indicate the timely entry of the prescription, it remains a product generated under the control of the data provider and therefore does not, by itself, provide independent verification of the origin, completeness, and conditions under which the information was generated. This is where the limitation of the independence criterion becomes apparent.

Accessing technical layers of data—audit logs, version history, and intersystem events—can significantly alter the reconstruction of circumstances. At this level, it may become apparent that a record was modified later, retransmitted, confirmed with a delay, or became visible in another subsystem at a different time than predicted by the human-readable document. Consequently, without access to these layers of the digital trail, a reliable reconstruction of the chronology is impossible, making the sufficiency criterion central to assessing the evidentiary quality of the data.

Even a potentially complete data set retains its evidentiary value only if it is preserved in a timely manner. Limited log retention periods, automatic overwriting, and the lack of emergency retrieval mechanisms can lead to the loss of critical information even before a full analysis can begin. This is where the importance of the timeliness criterion comes into play: it answers the question of whether it is even possible to preserve a digital trace before it disappears.

Finally, the mere availability of data does not guarantee its evidentiary validity without the ability to independently verify the expert analysis. Such verification

requires preserving the original dataset, documenting the extraction and processing procedures, and ensuring transparency of the analytical steps. Only when these conditions are met is the reproducibility criterion met, allowing for repeated testing and verification of the findings.

Taken together, the proposed test demonstrates that limiting an investigation solely to a report generated by a medical organization creates a high risk of distorting the actual picture. Conversely, consistent adherence to the criteria of independence, sufficiency, timeliness, and reproducibility transforms the digital sequence of events from a formal set of records into a verifiable and evidentiary reliable object of analysis.

In a broader analytical sense, the test distinguishes between digital maturity and evidentiary maturity. A high degree of digitalization alone does not guarantee the reliability of the evidentiary base: even technologically advanced systems may exhibit limitations in terms of independence or timeliness if logs are retained for a limited time or data retrieval remains under the control of the provider. At the same time, a less developed digital environment can improve its evidentiary strength through effective data preservation procedures, standardized retrieval protocols, and interdisciplinary expert practices.

This logic is further reflected in the comparative profile presented in Table 3. This profile is illustrative and interpretive in nature. Its purpose is not to quantitatively evaluate systems, but to analytically identify typical institutional bottlenecks that arise when working with electronic medical data in different jurisdictions.

Table 3. Illustrative analytical profile of selected jurisdictions (non-empirical comparison).

Jurisdiction	Independence	Sufficiency	Timeliness	Reproducibility	Indicative profile
France	Moderate	Moderate	High	Moderate	Institutionally documented, digitally partial
Germany	Moderate	Moderate	High	Moderate	Expert-strong, digitally partial
United Kingdom	High	Moderate	High	Moderate	Independent safety review, evidentiary-conversion gap
United States	Moderate	High	Moderate	Moderate	Digitally advanced, structurally heterogeneous
Romania	Low	Moderate	Moderate	Low	Procedure-led, infrastructure-forming
Moldova	Low	Low	Moderate	Low	High dependence on provider-controlled evidence
Ukraine	Low	Low	Moderate	Low	Procedure-led, uneven digital preservation

Note: The profile is illustrative and interpretative. It is based on doctrinal and institutional materials reviewed in this article and does not rely on an empirical dataset of cases or outcomes. It should not be read as a validated ranking, measurement, or comparative performance assessment.

3.7.1. Scenario-based analytical illustration of the functional test: United States and Moldova

To demonstrate the operational value of the proposed model, a typical hypothetical scenario of a potential delay in the administration of a critically important drug is considered below. In this scenario, the key is to reconstruct the sequence of actions—prescription, transfer, confirmation, and administration. This

example is used solely as a scenario-analytical illustration of the functional test's operation in various institutional settings. It is not based on a specific empirical case and should not be considered a description of a real-world case.

In such a situation, a human-readable entry in an electronic medical record can create the appearance of timeliness in the actions of medical personnel. However, a legally significant reconstruction depends not only on the content of such an entry, but also on the analysis of metadata, audit logs, change history, and intersystem events. Consequently, evidentiary assessment is determined not only by the content of the document, but primarily by the structure of the digital trace and the institutional conditions for its storage, retrieval, and analysis.

In the institutional configuration of the United States, this scenario allows us to analytically describe the combination of high digital maturity and heterogeneous evidence-based practices. Modern healthcare information systems are capable of generating detailed audit trails and other technical data layers potentially suitable for event reconstruction. However, access to this data is provided through formally established but variable procedures and, in practice, often remains mediated by the healthcare organization or system provider. As a result, significant digital potential does not always translate into evidentiary reliability: retrieval procedures can be heterogeneous, timeliness of preservation depends on procedural dynamics, and reproducibility of analysis is limited by the lack of uniform requirements for documenting technical operations.

In terms of a functional test, such a configuration can be analytically characterized as a conditional profile: independence - 1-2, sufficiency - 2, timeliness - 1-2, reproducibility - 1. This characteristic is interpretive in nature and is based on normative and institutional materials, and not on a structured empirical sample of cases.

In the case of the Republic of Moldova, the analytical picture is constructed differently. The main limitations are primarily related to the dependence on controlled data sources. Access to digital information is largely determined by the cooperation of medical institutions and their technical capabilities, which creates the risk of the formation of an evidentiary body under the control of a potentially interested party. Available data is often limited to human-readable records or incomplete technical layers, while comprehensive audit logs, change histories, and other elements of the digital footprint are either absent or not extracted in a procedurally relevant and verifiable form. The lack of developed mechanisms for operational preservation increases the risk of data loss, and expert analysis may ultimately rely on an incomplete and difficult-to-reproduce information base.

In the logic of a functional test, such a configuration can be analytically represented as a profile: independence - 0, sufficiency - 0-1, timeliness - 1, reproducibility - 0. This assessment reflects an analytical reading of available legal and institutional sources and is not an empirical measurement of the functioning of the system.

A comparison of these configurations reveals that the functional test does not capture the abstract level of "development" of a system or the degree of digitalization *per se*, but rather the specific conditions under which digital data acquires or loses evidentiary value. The differences between the systems are not linear, but structural: in some cases, limitations arise primarily at the level of procedural independence and reproducibility with high technological sophistication, while in others, they arise at the level of the very accessibility, completeness, and integrity of the digital trace.

This scenario-analytical illustration thus confirms the key thesis of the article: the reliability of electronic medical data is not an intrinsic or automatically inherent property. It is formed as a result of the coherence of the forensic infrastructure—digital, procedural, expert, and judicial—within which the data is created, stored, retrieved, interpreted, and evaluated.

4. Discussion

The main contribution of this article is the integration of several research areas—medical law, patient safety, digital forensics, and procedural standards for effective investigation—into a single analytical framework that allows for the evidentiary reliability of electronic medical data to be considered as a systemic property. Unlike approaches that focus primarily on individual elements—the clinical content of records, technical integrity of data, or procedural safeguards—the proposed model allows for the analysis of their interrelationships and the identification of structural conditions under which digital information gains or loses evidentiary value.

This approach allows us to reframe one of the most common issues in discussing medical incidents. Issues of medical negligence traditionally center around the standard of care and the quality of forensic evidence. Issues of digital evidence, by contrast, typically focus on the integrity, acquisition process, and chain of custody of data. In reality, in medical crime investigations, these dimensions do not exist in isolation. They intersect. A clinical opinion may be unreliable if it is based on a technically reduced or incomplete dataset; in turn, technically correct information extraction may be of limited value if the medical meaning of the recorded events is not interpreted in the proper clinical context.

The comparative analysis also shows that it's not so much the formal legal qualifications that are crucial, but the institutional architecture of the investigation. Legal systems may differ in the mechanism they place at the center of their response to medical incidents—compensatory, disciplinary, criminal, or based on independent patient safety investigations. However, the key evidentiary question remains the same: is the relevant system capable of preserving, obtaining, analyzing, and evaluating the relevant digital trace in a manner that is both lawful and verifiable? If the answer is no, not only the explanatory power of the investigation is weakened, but also its legitimacy.

The issue of trust is of additional significance in this context. Paper documentation could also be incomplete, inaccurate, or susceptible to manipulation. However, the digital environment increases the volume of technically hidden information and simultaneously concentrates practical control over this information in the hands of medical organizations and software solution providers. If the legal system lacks compelling mechanisms for independent data preservation and retrieval, doubts about the completeness and reliability of the evidence base become not random but structurally predictable. Consequently, the problem extends beyond the technical organization of document flow and touches upon the legitimacy of the state's response to serious harm in the medical field.

With increasing cyber risks and the increasing complexity of medical information system architectures, this problem is becoming systemic. It stems not only from the vulnerability of the data itself, but also from the difficulty of externally verifying how the digital trace was created, stored, and submitted for procedural assessment.

In addition, current international and interstate guidelines for handling electronic evidence emphasize that the admissibility and evidentiary value of digital data require independent assessment related to their origin, integrity, proper method of acquisition, and the possibility of subsequent verification.

From this perspective, the proposed model appears particularly useful in at least two ways. First, it can be used as an analytical framework for legal research and doctrinal rethinking of medical incident investigations in the context of digitalization. Second, it can serve as a practical guide for legislators, investigative bodies, medical institutions, and expert organizations interested in improving evidentiary preparedness without conflating this objective with an overly punitive approach. The proposed framework does not resolve all doctrinal issues, but it does

allow for the identification of those points at which evidentiary inconsistencies are most likely to arise.

The discussion thus confirms the article's main thesis: the reliability of electronic medical data is not an intrinsic quality of the record itself, but a result of the consistency of the digital, procedural, expert, and judicial environments. It is this consistency that determines whether the data can function as verifiable evidence in medical crime investigations.

5. Limitations

This study has a number of limitations arising from its doctrinal, comparative and analytical nature.

Firstly, this work is not an empirical study. It is based on an analysis of regulations, judicial practice, institutional materials, professional standards, and academic literature. The study did not include an analysis of a structured set of criminal cases, court decisions, or expert opinions in the jurisdictions under consideration. Accordingly, the findings are analytical propositions rather than empirically confirmed patterns.

Second, the selected jurisdictions are illustrative, not exhaustive. They were chosen to represent different institutional configurations and approaches to medical incident investigation, not to ensure statistical representativeness or generalizability of the results to a broader range of jurisdictions. Within each of the systems examined, significant variations are possible, particularly in decentralized healthcare models such as those found in the United States.

Third, the digital healthcare infrastructure is highly dynamic. Logging practices, data retention periods, information system architecture, interoperability standards, and regulatory requirements can change faster than scientific and legal literature can be compiled and updated. Therefore, any comparative conclusions regarding evidence readiness are provisional and require periodic review.

Fourth, the proposed forensic infrastructure model and investigative readiness test are heuristic in nature and are used as tools for analytical understanding and identification of institutional bottlenecks. They are not intended for quantitative measurement, do not generate validated indicators, and do not imply ranking of legal systems or assessing their effectiveness in a strictly empirical sense.

In this regard, further research could be aimed at empirically testing the proposed model. This testing could include a retrospective analysis of criminal cases, a structured analysis of court decisions and expert opinions, as well as expert interviews and scenario-based studies. Such approaches will allow us to assess the explanatory and practical potential of the model in specific law enforcement situations.

Thus, the limitations of the study reflect not shortcomings, but rather the limits of applicability of the chosen methodological approach. They emphasize that the presented findings should be viewed as an analytical basis for further theoretical and empirical development, rather than as definitive or universally generalizable results.

6. Recommendations

The recommendations formulated from the proposed forensic infrastructure model are aimed at improving the evidentiary value of electronic medical data by creating an auditable environment. Regulations should establish requirements for forensic readability of information systems, including logging, timestamp synchronization, maintaining change history, recording intersystem transactions, and exporting data with metadata. A significant condition is the availability of procedural mechanisms for the prompt preservation of data, allowing for its

recording before loss or modification. At the same time, it is necessary to reduce the reliance of investigations on information provided by medical organizations through the development of independent or procedurally controlled data extraction. Expert practice should be based on the interdisciplinary integration of forensic medicine and digital forensics with the standardization of methods and the structure of conclusions. Judicial practice requires a clearer articulation of criteria for evaluating digital evidence, including its origin, integrity, completeness, and reproducibility. Overall, improved evidentiary reliability is achieved through the coordinated development of technological, procedural, expert, and judicial mechanisms.

Taken together, these measures confirm that increased evidentiary reliability is achieved through the coordinated development of digital, procedural, expert and judicial mechanisms.

7. Conclusion

The digitalization of healthcare has significantly transformed the evidentiary environment for medical crime investigations. Modern systems capture not only clinical content but also metadata, audit logs, and intersystem interactions, expanding the possibilities for event reconstruction. At the same time, new risks arise related to limited transparency, data loss, and reliance on controlled sources.

The analysis shows that it's not digitalization itself that's crucial, but the state of the forensic infrastructure. Electronic medical data can only function as reliable evidence if conditions are in place that ensure traceability of its origin, timely receipt, complete retrieval, and the possibility of independent verification.

The article proposes a four-level infrastructure model and a functional test of investigative readiness based on the criteria of independence, sufficiency, timeliness, and reproducibility. These tools enable the identification of institutional constraints and the analysis of the conditions for the evidentiary suitability of data.

The key conclusion is that the evidentiary reliability of electronic medical data is a systemic property. It is shaped not by the content of the record, but by the conditions under which it is created, stored, retrieved, and evaluated. Without consistency among these elements, even a technologically advanced digital environment may fail to provide the required level of evidentiary validity.

In a broader context, the results highlight the need to integrate legal, technical, and expert approaches when organizing medical incident investigations. Further research could be aimed at empirically validating the proposed model and its application in law enforcement practice.

8. References

AL MAMUN, A.; AZAM, S.; GRITTI, C. "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction", IEEE Access, vol. 10, 2022, p. 5768–5789. https://doi.org/10.1109/ACCESS.2022.3141079

BOWMAN S. "Impact of electronic health record systems on information integrity: quality and safety implications", Perspectives in Health Information Management, 2013, vol. 10 (Fall), 1c. Available at: https://pubmed.ncbi.nlm.nih.gov/24159271/ (accessed on 12 January 2026).

CASEY E. "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet", 3rd ed., Waltham, MA: Academic Press, 2011. Available at: https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf (accessed on 12 January 2026).

CASEY E., BARNUM S., GRIFFITH R., SNYDER J., VAN BEEK H., NELSON A. "Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language", Digital Investigation, 2017, vol. 22, pp. 14–45. https://doi.org/10.1016/j.diin.2017.08.002

CHEN B., ALRIFAI W., GAO C., JONES B., NOVAK L., LORENZI N., FRANCE D., MALIN B.,

CHEN Y. "Mining tasks and task characteristics from electronic health record audit logs with unsupervised machine learning", Journal of the American Medical Informatics Association, 2021, vol. 28(6), pp. 1168–1177. https://doi.org/10.1093/jamia/ocaa338

D'ANNA T., PUNTARELLO M., CANNELLA G., SCALZO G., BUSCEMI R., ZERBO S., ARGO A. "The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data", Healthcare, 2023, vol. 11(5), p. 634. https://doi.org/10.3390/healthcare11050634

DETTMEYER R. B.; VERHOFF M. A.; SCHÜTZ H. F. "Forensic Medicine: Fundamentals and Perspectives". Berlin, Heidelberg: Springer, 2014. https://doi.org/10.1007/978-3-642-38818-7

EUROPEAN COURT OF HUMAN RIGHTS. Case of Arskaya v. Ukraine, no. 45076/05, 2013. Available at: https://hudoc.echr.coe.int/eng?i=001-138590 (accessed on 12 January 2026).

EUROPEAN COURT OF HUMAN RIGHTS. Case of Calvelli and and Ciglio v. Italy, no. 32967/96. 2002. Available at: https://hudoc.echr.coe.int/eng?i=001-60329 (accessed on 12 January 2026).

EUROPEAN COURT OF HUMAN RIGHTS. Case of Lopes de Sousa Fernandes v. Portugal, no. 56080/13. 2017. Available at: https://hudoc.echr.coe.int/eng?i=001-179556 (accessed on 12 January 2026).

EUROPEAN COURT OF HUMAN RIGHTS. Case of Šilih v. Slovenia, no. 71463/01. 2009. Available at: https://hudoc.echr.coe.int/fre?i=001-92142 (accessed on 12 January 2026).

EUROPEAN COURT OF HUMAN RIGHTS. Case of Tretyakova v. Ukraine, no. 63126/13, 2021. Available at: https://hudoc.echr.coe.int/eng?i=001-212963 (accessed on 12 January 2026).

EUROPEAN COURT OF HUMAN RIGHTS. Cauza Eugenia Lazăr v. Romania, no. 32146/05, 2010. Available at: https://hudoc.echr.coe.int/eng?i=001-123214 (accessed on 12 January 2026).

EUROPEAN UNION. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance). Official Journal of the European Union, 2025. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0327 (accessed on 12 January 2026).

FRANCE. Code de la santé publique, art. L1111-7. Paris: Legifrance, current version. Available at: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042685313 (accessed on 12 January 2026).

FRANCE. Code de procédure pénale. Paris: Legifrance, current version. Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154 (accessed on 12 May 2026).

FRANCE. Code pénal. Paris: Legifrance, current version. Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719 (accessed on 12 May 2026).

GERMANY. Bürgerliches Gesetzbuch (BGB), 630f–630g. Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/bgb/index.html#BJNR001950896BJNE271701360 (accessed on 12 January 2026).

GERMANY. Sozialgesetzbuch V (SGB V), 342. Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/sgb_5/index.html#BJNR024820988BJNE079305126 (accessed on 12 January 2026).

GERMANY. Sozialgesetzbuch V (SGB V), 355. Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/sgb_5/index.html#BJNR024820988BJNE080606126 (accessed on 12 January 2026).

GERMANY. Strafprozessordnung (StPO). Berlin: Federal Ministry of Justice of Germany, current version. Available at: https://www.gesetze-im-internet.de/stpo/ (accessed on 12 January 2026).

ISO/IEC. ISO/IEC 27037:2012 – Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: International Organization for Standardization, 2012. Available at: https://www.iso.org/standard/44381.html (accessed on 12 January 2026).

KENT K.; CHEVALIER S.; GRANCE T.; DANG H. "Guide to Integrating Forensic Techniques

into Incident Response". NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology, 2006. Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf (accessed on 12 January 2026).

KOHN L. T.; CORRIGAN J. M.; DONALDSON M. S. (eds.). "To Err Is Human: Building a Safer Health System", Washington, DC: National Academies Press, 2000. https://doi.org/10.17226/9728

MERRY A. F.; BROOKBANKS W. "The Place of the Criminal Law in Healthcare", in: MERRY A. F.; MCCALL SMITH A. (eds.), Errors, Medicine and the Law, 2nd ed., Cambridge: CUP, 2017, pp. 310–345. https://doi.org/10.1017/9781316848050.011

REPUBLIC OF MOLDOVA. Codul de procedură penală al Republicii Moldova nr. 122-XV din 14 martie 2003. Chișinău: Legis.md, current version. Available at: https://www.legis.md/cautare/getResults?doc_id=154997⟨=ro (accessed on 12 January 2026).

REPUBLIC OF MOLDOVA. Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Chișinău: Legis.md, current version. Available at: https://www.legis.md/cautare/getResults?doc_id=148996⟨=ro# (accessed on 12 January 2026). At the date of this study, Law No. 133/2011 remained applicable in the Republic of Moldova; however, it was scheduled to be repealed and replaced by Law No. 195/2024 on 23 August 2026.

REPUBLIC OF MOLDOVA. Legea nr. 411-XIII din 28 martie 1995 privind ocrotirii sănătății. Chișinău: Legis.md, current version. Available at: https://www.legis.md/cautare/getResults?doc_id=151100⟨=ro (accessed on 12 January 2026).

ROMANIA. Codul de procedură penală (Legea nr. 135/2010). Bucharest: Portal Legislativ, current version. Available at: https://legislatie.just.ro/Public/DetaliiDocument/210279 (accessed on 12 January 2026).

ROMANIA. LEGE nr. 95 din 14 aprilie 2006 privind reforma în domeniul sănătății. Bucharest: Portal Legislativ, current version. 2015. Available at: https://legislatie.just.ro/Public/DetaliiDocument/71139 (accessed on 12 January 2026).

ROMANIA. LEGEA drepturilor pacientului nr. 46 din 21 ianuarie 2003. Bucharest: Portal Legislativ, current version. Available at: https://legislatie.just.ro/Public/DetaliiDocument/296139 (accessed on 12 January 2026).

RULE A., KANNAMPALLIL T., HRIBAR M. R., DZIORNY A. C., THOMBLEY R., APATHY N. C., ADLER-MILSTEIN J. "Guidance for reporting analyses of metadata on electronic health record use", Journal of the American Medical Informatics Association, 2024, vol. 31(3), pp. 784–789. https://doi.org/10.1093/jamia/ocad254

RULE A.; CHIANG M. F.; HRIBAR M. R. "Using electronic health record audit logs to study clinical activity: a systematic review of aims, measures, and methods", Journal of the American Medical Informatics Association, 2020, vol. 27(3), pp. 480–490. https://doi.org/10.1093/jamia/ocz196

TABARI, P.; COSTAGLIOLA, G.; DE ROSA, M.; BOEKER, M. "State-of-the-Art Fast Healthcare Interoperability Resources (FHIR)–Based Data Model and Structure Implementations: Systematic Scoping Review", JMIR Medical Informatics, vol. 12, 2024, e58445. https://doi.org/10.2196/58445

UKRAINE. CABINET OF MINISTERS. Деякі питання електронної системи охорони здоров'я [Some Issues of the Electronic Health Care System]: Resolution No. 411 of 25 April 2018, revision of 4 February 2025. Legislation of Ukraine database / Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/411-2018-%D0%BF (accessed on 12 January 2026).

UKRAINE. MINISTRY OF HEALTH. Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я [Some issues relating to the maintenance of the Register of medical records, referral records and prescriptions in the electronic healthcare system]: Order No. 587 of 28 February 2020; registered by the Ministry of Justice of Ukraine on 5 March 2020 under No. 236/34519; revision of 21 November 2025. Legislation of Ukraine database / Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/z0236-20 (accessed on 12 January 2026).

UKRAINE. The Criminal Procedural Code of Ukraine: Code of Ukraine, Law No. 4651-VI of 13 April 2012, revision of 1 August 2025. Legislation of Ukraine database / Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/4651-17 (accessed on 12 January

2026).
UNITED KINGDOM. Data Protection Act 2018. London: legislation.gov.uk, current version. Available at: https://www.legislation.gov.uk/ukpga/2018/12 (accessed on 12 January 2026).
UNITED KINGDOM. Health and Care Act 2022. London: legislation.gov.uk, current version. Available at: https://www.legislation.gov.uk/ukpga/2022/31 (accessed on 12 January 2026).
UNITED KINGDOM. Police and Criminal Evidence Act 1984. London: legislation.gov.uk, current version. Available at: https://www.legislation.gov.uk/ukpga/1984/60 (accessed on 12 January 2026).
UNITED STATES. 21st Century Cures Act; ONC Certification Criteria (45 CFR § 170.315). Washington, DC: Office of the National Coordinator for Health Information Technology, current version. Available at: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-170/section-170.315 (accessed on 12 January 2026).
UNITED STATES. Federal Rules of Criminal Procedure, Rule 41. Washington, DC: United States Courts, current version. Available at: https://www.law.cornell.edu/rules/frcrmp/rule_41 (accessed on 12 January 2026).
UNITED STATES. Health Insurance Portability and Accountability Act (HIPAA), 45 CFR § 164.312. Washington, DC: Electronic Code of Federal Regulations, current version. Available at: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312 (accessed on 12 January 2026).
UNITED STATES. Health Insurance Portability and Accountability Act (HIPAA), 45 CFR § 164.512(f). Washington, DC: Electronic Code of Federal Regulations, current version. Available at: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.512 (accessed on 12 January 2026).
VULETIĆ, I. "Medical Malpractice as a Separate Criminal Offense: A Higher Degree of Patient Protection or Merely a Sword Above the Doctors' Heads? The Example of the Croatian Legislative Model and the Experiences of its Implementation", Medicine, Law & Society, 12(2), 2019, pp. 39-60. https://doi.org/10.18690/10.18690/mls.12.2.39-60.2019
WASSERMAN L.; WASSERMAN Y. "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)", Frontiers in Digital Health, 2022, vol. 4, 862221. https://doi.org/10.3389/fdgth.2022.862221
WORLD HEALTH ORGANIZATION. Global Patient Safety Action Plan 2021–2030: Towards Eliminating Avoidable Harm in Health Care. Geneva: WHO, 2021. Available at: https://iris.who.int/handle/10665/343477 (accessed on 12 January 2026).