Degree project

UNIVERSITY
OF SKÖVDE

Digital Forensic Readiness Models and Frameworks in the Healthcare Sector: Supporting Compliance, Accountability, and Cyber Resilience

Bachelor Degree Project in Informatics

First Cycle 30 credits

Spring term 2026

Student: Mohamud Ismail

Supervisor: Muhammad Abbas Khan Abbasi

Examiner: Thomas Fischer

Acknowledgement

I would like to thank my supervisor and examiner, Muhammad Abbas Khan Abbasi and Thomas Fischer, for their guidance and support throughout this project. I would also like to thank my family and friends for their support, encouragement, and understanding during the completion of this study.

Abstract

Digital Forensic Readiness (DFR) models and frameworks allow organisations to prepare their systems so that digital evidence can be collected, preserved and used after a security incident. They specify what should be logged, how evidence should be protected against alteration, and who is responsible for handling it before a breach occurs. This capability is particularly relevant to healthcare organisations, which hold sensitive patient data and depend on the continuous availability of clinical systems.

This study examines which requirements related to compliance, accountability and cyber resilience within the Swedish healthcare sector are supported by existing DFR models and frameworks, and which gaps remain. Nine requirements were derived from the General Data Protection Regulation (Regulation 2016/679), the Network and Information Security 2 Directive (Directive 2022/2555), the Cyber Resilience Act (Regulation 2024/2847), the European Health Data Space Regulation (Regulation 2025/327), the Swedish Patient Data Act (SFS 2008:355), and the National Board of Health and Welfare′s regulations on record-keeping and the processing of personal data in healthcare (HSLF-FS 2016:40). A structured literature review was conducted across seven databases, resulting in fifteen included studies. Each study was analysed against the nine requirements using a coding framework defined before analysis, with every coding decision supported by a passage from the reviewed article.

The findings show varying levels of support. Within the compliance dimension, evidence preservation receives the strongest support, with direct evidence in thirteen of fifteen studies; data minimisation is addressed by four studies, and protection of patients as data subjects by seven. Accountability is the best-supported dimension: the logging and monitoring requirement is addressed by fourteen studies and traceability by eleven, although four studies do not specify a responsible party. Cyber resilience is the least-supported dimension, with risk management and operational continuity each addressed by five studies.

No reviewed approach derives its requirements from health-sector legal obligations, engages with health-sector interoperability standards, or has been implemented in an operational healthcare setting. The results therefore describe what these approaches specify rather than what they achieve in practice.

Keywords: digital forensic readiness, healthcare sector, compliance, accountability, cyber resilience

Contents

1 Introduction **1**

1.1 Aims . . . 1

2 Background **2**

2.1 Preliminaries and Concepts . . . 2

2.1.1 The Digital Transformation in the Healthcare Sector . . . 2

2.1.2 The Cybersecurity Threat Landscape in the Healthcare Sector . . . 3

2.1.3 Digital Forensics and Digital Forensic Readiness . . . 4

2.1.4 Compliance, Accountability, and Cyber Resilience . . . 5

2.2 Research background . . . 9

2.2.1 Foundational Digital Forensic Readiness Models . . . 9

2.2.2 Existing Literature . . . 10

3 Problem formulation **12**

3.1 Study aims . . . 12

3.2 Research Question and Guidance Questions . . . 13

3.3 Motivation . . . 13

3.4 Delimitations . . . 14

4 Methodology **15**

4.1 Data collection . . . 16

4.1.1 Two Retrieval Routes . . . 16

4.1.2 Database and Search String . . . 16

4.1.3 Inclusion and Exclusion Criteria . . . 17

4.1.4 Screening . . . 17

4.1.5 Study Selection . . . 17

4.2 Data analysis . . . 18

4.2.1 Analytical Approach . . . 18

4.2.2 Data Extraction . . . 19

4.2.3 Coding Framework . . . 19

4.2.4 Synthesis . . . 20

4.3 Validity and Reliability . . . 20

4.4 Ethical Aspects . . . 20

5 Results **22**

5.1 Characteristics of the Included Studies 23

5.2 Compliance Requirements 25

5.2.1 Data Protection and Privacy 25

5.2.2 Interoperability and Technical Standards 26

5.2.3 Evidence Preservation and Data Minimisation 26

5.3 Accountability Requirements 27

5.3.1 Logging and Monitoring 28

5.3.2 Responsibility and Governance 28

5.3.3 Traceability and Identification 29

5.4 Cyber Resilience Requirements 30

5.4.1 Risk Management 30

5.4.2 Operational Continuity and Preparedness 31

5.4.3 Incident Response and Recovery 31

5.5 Healthcare-Specific and General Forensic Readiness Compared 32

5.6 Synthesis 33

5.6.1 Recurring Patterns Across the Included Studies 33

5.6.2 Differences in Emphasis Between Approaches 33

5.6.3 Complementary Capabilities 34

5.6.4 Healthcare-Specific Characteristics 34

5.6.5 Overall Findings 35

5.6.6 Remaining Gaps 35

6 Discussion **37**

6.1 In relation to previous research . . . 37

6.1.1 Relation to the Conceptual Framework . . . 37

6.1.2 Relation to Previous Digital Forensic Readiness Research . . . 38

6.1.3 Relation to Healthcare Cybersecurity Research . . . 38

6.2 Ethical and societal aspects . . . 39

6.2.1 Forensic Readiness in Healthcare Is a Form of Workplace Monitoring . . . 39

6.2.2 The Minimisation Gap Has Consequences for Patients . . . 39

6.2.3 Designing Around the Insider Affects Trust . . . 40

6.2.4 Capability Is Not Distributed Equally . . . 40

6.2.5 Relation to the Sustainable Development Goals . . . 41

7 Conclusion **42**

7.1 Contribution . . . 43

7.2 Future work . . . 43

References **44**

A Retrieval of legal and regulatory instruments **48**

B Evidence extraction record **49**

B.1 S1 – Chernyshev, Zeadally and Baig (2019) . . . 50

B.2 S2 – Grispos, Glisson and Choo (2017) . . . 51

B.3 S3 – Yaqub, Jo, Nadeem, Topsakal and Ahmed (2026) . . . 52

B.4 S4 – Mpungu, George and Mapp (2024) . . . 53

B.5 S5 – Mishra and Bagade (2022) . . . 54

B.6 S6 – Al-Balasmeh (2026) . . . 55

B.7 S7 – Zehra, Javed, Hyder, Darakhshan and Tariq (2024) . . . 56

B.8 S8 – Kyaw, Cusack and Lutui (2019) . . . 57

B.9 S9 – Kyaw, Tian and Cusack (2020) . . . 58

B.10 S10 – Cusack and Kyaw (2012) . . . 59

B.11 S11 – Gombar, Možnik and Pejić Bach (2026) . . . 60

B.12 S12 – Mekala, Baig, Anwar, Syed and Zeadally (2025) . . . 61

B.13 S13 – Adel, Ahsan and Davison (2024) 62
B.14 S14 – Bankole, Taiwo and Claims (2022) 63
B.15 S15 – Janjua, Shah, Almogren, Khattak, Maple and Din (2020) 64

C Evidence matrix and distribution summary **65**

1 Introduction

Healthcare organisations hold some of the most sensitive personal data and depend heavily on digital systems to deliver care. These characteristics make the sector attractive to attackers and increase the consequences of an attack (Shahzadi et al., 2025). While an attack on a commercial organisation may cause financial and reputational damage, an attack on a hospital can also interrupt patient treatment (Kruse et al., 2017; Moore et al., 2023).

When an incident occurs, an organisation needs to establish what happened, which systems and records were affected, and who was responsible. Answering these questions requires digital evidence, and that evidence must exist before it can be examined. If the necessary records were never captured, were overwritten, or cannot be shown to be unaltered, an investigation may remain inconclusive regardless of the expertise applied.

Digital forensic readiness (DFR) addresses this by preparing for investigation before an incident occurs. Rowlingson (2004) defines forensic readiness as an organisation's ability to maximise the potential use of digital evidence while minimising the cost of an investigation, framing it as a corporate goal rather than a technical activity. Pangalos and Katos (2010, as cited in Englbrecht et al., 2020) extend this by describing readiness as a state in which controls are in place to facilitate the forensic process and anticipate unauthorised actions that could disrupt planned operations. A DFR model or framework provides a structured description of how an organisation achieves this. In practice, it specifies which systems and events should be logged and what those logs must contain, how collected evidence is protected against alteration, who is responsible for handling it, and when an incident should be escalated to a formal investigation.

Healthcare organisations operate under obligations that make this capability directly relevant. Data concerning health are included among the special categories of personal data in Article 9(1) of the General Data Protection Regulation (Regulation 2016/679). The Network and Information Security 2 Directive (Directive 2022/2555) lists health as a sector of high criticality in Annex I, point 5, including healthcare providers. Which organisations fall within the Directive and whether they are classified as essential or important entities is determined by Articles 2 and 3. For entities within scope, Article 21 establishes cybersecurity risk-management requirements and Article 23 establishes reporting obligations for significant incidents. In Sweden, the Swedish Patient Data Act (SFS 2008:355), Chapter 4, Section 3, requires care providers to ensure that automated access to patient data is documented and can be checked, and to conduct systematic and recurring checks for unauthorised access.

A substantial number of DFR models and frameworks have been proposed in the research literature. They differ in the environments they address, whether they emphasise organisational processes or technical mechanisms, and how extensively they have been evaluated. What remains unclear is how well these approaches correspond to the obligations that apply to healthcare organisations operating under Swedish and European law.

1.1 Aims

This study aims to compare existing digital forensic readiness models and frameworks against the requirements for compliance, accountability and cyber resilience that apply to the Swedish healthcare sector, and to identify where those requirements are not supported. The requirements derive from Swedish and European Union legal and regulatory instruments, as Swedish care providers are governed by both national and Union rules.

2 Background

This chapter contains the background needed to understand the context of the study. Section 2.1 presents the fundamental concepts: the digital transformation of the healthcare sector, the cybersecurity threat landscape, digital forensics and digital forensic readiness, and the three dimensions of compliance, accountability and cyber resilience together with the specific requirements derived from them. Section 2.2 presents the DFR models and frameworks proposed in the research literature, which provide the basis against which those requirements are compared in Chapter 5.

2.1 Preliminaries and Concepts

This subsection introduces the concepts needed to understand the study: the digital transformation of healthcare, the healthcare cybersecurity threat landscape, digital forensics and digital forensic readiness, and the compliance, accountability and cyber resilience requirements used in the analysis.

2.1.1 The Digital Transformation in the Healthcare Sector

Electronic Health Records (EHRs) are among the most important components of modern digital healthcare systems. An EHR is a digitalised version of a patient's medical history, maintained by healthcare providers over time, and includes information such as patient diagnoses, demographics, medications, treatment plans, laboratory results, radiology images and clinical notes (Office of the National Coordinator for Health Information Technology [ONC], 2025). The EHR is the point at which much clinical activity becomes recorded data and, consequently, the point at which many questions about access to patient information must be answered.

The healthcare sector has transformed rapidly over the past two decades through the adoption of EHRs, wireless medical devices and interconnected information systems to improve patient care, operational efficiency and real-time decision-making. The integration of digital technologies has enabled hospitals to make use of remote diagnostics, continuous patient monitoring and streamlined administrative processes.

Healthcare infrastructure consists of physical, technological and organisational components that support the delivery of healthcare services. According to Chernyshev et al. (2019), modern healthcare infrastructure includes hospital information systems such as EHR platforms, medical imaging systems, clinical decision-support systems, cloud storage environments and interconnected medical devices, including infusion pumps, heart monitors and wearable health sensors. EHR systems also allow healthcare providers to share patient information across healthcare institutions and departments. This interoperability supports better care and enables patient information to be used for performance feedback (Adler-Milstein et al., 2017).

Digital transformation is also extending beyond individual healthcare providers. According to the Swedish eHealth Agency (E-hälsomyndigheten, 2025), the Swedish government has worked to transform the national healthcare sector through a National Digital Infrastructure (Nationell digital infrastruktur, NDI). The initiative began implementation in 2025, with the aim that certain categories of health data will be required to be shared nationally and across European Union borders by March 2029. These categories include electronic prescriptions, patient summaries and electronic dispensations. The initiative is intended to increase the quality of healthcare, improve patient safety and support healthcare administration. At the European Union level, this development is governed by the European Health Data Space Regulation (Regulation 2025/327), which establishes a framework for access to and exchange of electronic health data. The EHDS enables both the primary use of health data for the delivery of care and its secondary use

for research, innovation, policymaking and regulatory activities, subject to defined conditions (Regulation 2025/327).

Regulation (EU) 2025/327 establishes the European Health Data Space framework for access to, exchange of, and use of electronic health data. Personal electronic health data recorded in EHRs commonly include an individual's medical history, including diagnoses and treatments, medications, allergies and radiology images. The regulation aims to facilitate access to and the sharing of electronic health data among healthcare professionals and across member states. Some member states have taken legal and technical measures to establish centralised infrastructure connecting the EHR systems used by healthcare providers. Such infrastructure is intended to facilitate the free movement of personal electronic health data across the EU and reduce situations in which patients are unable to receive appropriate treatment when receiving healthcare in another member State.

The EHDS entered into force on 26 March 2025, marking the beginning of a transition period. Its provisions are being introduced in stages. By 26 March 2027, the European Commission is to adopt implementing acts establishing technical specifications for the priority categories of electronic health data. As the relevant provisions become applicable, the regulation is intended to support patients, healthcare professionals, researchers and policymakers across the EU (Regulation 2025/327).

The digitalisation of healthcare in Sweden is also governed by the Swedish Patient Data Act (SFS 2008:355), which supplements the GDPR for healthcare-sector processing and contains rules on patient records, internal confidentiality and electronic access.

2.1.2 The Cybersecurity Threat Landscape in the Healthcare Sector

The adoption of digital technologies in the healthcare sector has not been matched by a corresponding level of security readiness, which has made the sector a prominent target for cybercriminals. Patient data that combine personal, financial and medical information are valuable in illicit markets, increasing both the risk and the impact of breaches (Shahzadi et al., 2025). The sector has also been associated with fundamental security weaknesses such as device theft or loss, human error, ransomware attacks and insider misuse, rather than primarily with technological vulnerabilities (Verizon, 2018, as cited in Chernyshev et al., 2019).

The threat is not limited to data. Connected medical devices can themselves be affected by cybersecurity vulnerabilities. Islam et al. (2022) describe a 2017 case in the United States involving Abbott implantable cardiac pacemakers. The U.S. Food and Drug Administration issued a safety recommendation advising patients with affected devices to visit the nearest clinic to update their device firmware.

A comparable incident affecting an entire health service occurred in Ireland in 2021, when the Health Service Executive (HSE) was subjected to a Conti ransomware attack. Moore et al. (2023) explain that the attack caused the loss of ICT systems, forcing staff to use workarounds and paper-based systems to continue delivering care safely. According to the HSE's independent post-incident review, the attack began when a HSE workstation was infected with malware after its user opened a malicious Microsoft Excel file attached to a phishing email received on 16 March 2021. The infection itself occurred on 18 March 2021 (HSE, 2021, p. 2).

The attacker then operated inside the HSE's network for around eight weeks, compromising privileged accounts, exfiltrating data and moving laterally to hospitals connected to the National Healthcare Network before deploying the Conti ransomware in the early hours of 14 May 2021 (HSE, 2021, pp. 2–3). The HSE's incident response provider identified 180 compromised systems across eight organisations and 19 domains. Evidence of encryption was found on more than 2,800 servers and 3,500 workstations spanning 15 domains. HSE management separately estimated that around 80% of the organisation's

entire IT environment, spanning corporate systems, hospitals, community healthcare organisations and EHRs, had been encrypted (HSE, 2021, pp. 15, 45, 55).

Recovery took more than four months. Approximately 47% of servers had been decrypted one month after the attack, on 14 June 2021, and 94% had been decrypted by 20 July. Server decryption was complete by 17 August, while application restoration continued until around 21 September 2021, when approximately 99% of applications were back in service (HSE, 2021, pp. 3, 18). Clinical disruption was extensive. On the morning of the attack, 31 of the HSE's 54 acute hospitals cancelled at least some services, with disruption affecting outpatient clinics, diagnostic imaging, radiotherapy, certain pathology tests and elective surgeries. Community and primary care staff also lost electronic access to patient appointment lists and clinical histories. Emergency care and the National Ambulance Service, by contrast, continued to operate throughout (HSE, 2021, pp. 15, 20).

The distinction between these two incidents is relevant to this study. The Abbott case concerned a vulnerability in a medical device, whereas the HSE case concerned the operational continuity of an entire health service. Both required subsequent investigation, and in both cases the ability to investigate depended on what had been recorded beforehand.

The threat profile of the healthcare sector also differs from that of many other sectors in an important respect. Chernyshev et al. (2019) report that internal actors account for the majority of healthcare breach incidents and characterise their motives as personal gain, snooping and curiosity about the records of colleagues, neighbours, family members and high-profile individuals. This means that the person whose actions must be investigated is frequently an authorised user of the system rather than an external attacker who must first obtain access.

2.1.3 Digital Forensics and Digital Forensic Readiness

Digital forensics is the process of identifying, collecting, preserving and analysing digital evidence so that it remains valid for investigative and legal purposes. Traditionally, this process has been reactive, performed after an incident has been detected. Digital forensic readiness makes the process proactive. Rowlingson (2004) provides the original definition, describing forensic readiness as an organisation's ability to maximise the potential use of digital evidence while minimising the cost of an investigation. Although this definition is more than two decades old, it remains the basis for later work. Reddy and Venter (2013), Elyas et al. (2015), Grispos et al. (2017), Kebande and Venter (2019) and Englbrecht et al. (2020) all take it as their starting point. Gombar et al. (2026) adapt Rowlingson's ten-step process into survey indicators for empirical measurement.

Subsequent research has expanded the concept. Pangalos and Katos (2010, as cited in Englbrecht et al., 2020) add an anticipatory perspective, describing forensic readiness as a state in which controls are in place to facilitate the forensic process and to anticipate unauthorised actions that could disrupt planned operations. Tan (2001, as cited in Kebande & Venter, 2019) similarly frames the objectives as maximising an environment's ability to collect credible digital evidence while minimising the cost of conducting investigations. More recent work has extended readiness to specific environments, including regulated medical devices (Yaqub et al., 2026), wireless medical systems (Kyaw et al., 2019), the medical Internet of Things (Al-Balasmeh, 2026), and the derivation of readiness requirements from risk management (Daubner et al., 2023a).

In this study, the terms "model" and "framework" both describe structured approaches to digital forensic readiness. A framework can be understood as a network of interlinked concepts that together provide a structure for understanding a phenomenon (Jabareen, 2009). A model is a more concrete representation that describes the specific components and processes through which that structure is applied.

Carrier and Spafford (2004, as cited in Englbrecht et al., 2020) distinguish between two aspects of readiness. Operational readiness concerns providing adequate training and equipment for individuals involved in forensic activities. Infrastructural readiness concerns establishing the means by which evidence can be appropriately preserved. This distinction recurs throughout Section 2.2, where some approaches address the organisational dimension of readiness while others focus on the technical mechanisms that produce and protect evidence.

2.1.4 Compliance, Accountability, and Cyber Resilience

This section presents the three dimensions used in the analysis and the nine requirements derived from them. The legal basis comprises the General Data Protection Regulation (Regulation 2016/679), the Network and Information Security 2 Directive (Directive 2022/2555), the Cyber Resilience Act (Regulation 2024/2847), the European Health Data Space Regulation (Regulation 2025/327), the Swedish Patient Data Act (SFS 2008:355), and the National Board of Health and Welfare's regulations on record-keeping and the processing of personal data in healthcare (HSLF-FS 2016:40).

The EHDS Regulation, the Patient Data Act and HSLF-FS 2016:40 are healthcare-specific instruments. The GDPR is a cross-sectoral data protection regulation. NIS 2 is also cross-sectoral, but Annex I, point 5, expressly lists health as a sector of high criticality and includes healthcare providers; applicability and classification as an essential or important entity follow Articles 2 and 3 of the Directive (Directive 2022/2555). The EHDS entered into force in March 2025, but its substantive application is phased. Article 105 provides for general application from 26 March 2027, while Articles 3–15 apply to the first priority categories of personal electronic health data from 26 March 2029 and to the remaining priority categories from 26 March 2031 (Regulation 2025/327, Art. 105). The CRA is horizontal product legislation. Article 2(1) covers products with digital elements made available on the market whose intended purpose or reasonably foreseeable use includes a direct or indirect data connection, while Article 2(2)–(7) contains exclusions, including products governed by the EU medical-device and in-vitro diagnostic-device regulations (Regulation 2024/2847). At the study's Spring 2026 reference point, the CRA's general application date was still future: most provisions apply from 11 December 2027, while Article 14 reporting obligations apply from 11 September 2026 (Regulation 2024/2847, Art. 71(2)). Consequently, CRA criteria are used in this study only where they are relevant to products within the Regulation's scope, and with their application dates in mind.

Compliance

Compliance in this study concerns the legal and regulatory requirements that govern the processing and protection of health data and the handling of cybersecurity incidents. Article 9(1) of the GDPR includes data concerning health among the special categories of personal data whose processing is prohibited unless an exception in Article 9(2) applies. Article 9(2)(h) permits processing that is necessary for preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services, subject to the basis and safeguards stated there and the professional-secrecy condition in Article 9(3) (Regulation 2016/679, Art. 9(1)–(3)). Article 32(1) requires controllers and processors to implement technical and organisational measures appropriate to the risk, including, where appropriate, measures supporting confidentiality, integrity, availability and resilience. Article 33(1) requires a controller to notify a personal data breach to the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of people (Regulation 2016/679, Arts. 32(1), 33(1)).

For entities that fall within NIS 2, Article 21 requires member states to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational cybersecurity risk-management measures. Article 23 separately establishes staged reporting obligations for significant

incidents, including an early warning within 24 hours and an incident notification within 72 hours (Directive 2022/2555, Arts. 21(1)–(2), 23(1), 23(4)).

Three compliance requirements are derived for this study.

C1 Data protection and privacy.

The requirement combines the GDPR's protection of health data with healthcare-specific access safeguards. GDPR Article 5(1)(f) requires personal data to be processed with appropriate security against unauthorised or unlawful processing and accidental loss, destruction or damage, while Article 9 governs the processing of health data as a special category (Regulation 2016/679, Arts. 5(1)(f), 9). In Sweden, Chapter 1, Section 2 of the Patient Data Act requires healthcare information management to respect the privacy of patients and other data subjects and requires documented personal data to be handled and stored so that unauthorised persons cannot access them (SFS 2008:355, 1 kap. 2 §). The EHDS Regulation additionally establishes a right for natural persons to restrict health professionals' and healthcare providers' access to all or parts of their personal electronic health data, subject to the Regulation's detailed rules and possible emergency safeguards; that right applies according to the phased dates in Article 105 (Regulation 2025/327, Arts. 8, 105).

C2 Interoperability and technical standards.

The EHDS Regulation establishes a concrete interoperability framework for electronic health data, subject to the staged application dates in Article 105. Article 15(1) requires the Commission to lay down technical specifications for the European electronic health record exchange format for the priority categories in Article 14(1); the format must be commonly used, machine-readable and enable transmission between different software applications, devices and healthcare providers. Article 15(4) requires member states, once the relevant provisions apply, to ensure that those priority categories are issued in that format and that, when transmitted automatically for primary use, receiving healthcare providers accept and can read the format (Regulation 2025/327, Arts. 15(1), 15(4), 105). For EHR systems, Article 30(1)(a) requires manufacturers to ensure conformity with the essential requirements in Annex II and the common specifications adopted under Article 36. Annex II contains separate interoperability requirements and security-and-logging requirements for the harmonised software components of EHR systems (Regulation 2025/327, Art. 30(1)(a), Annex II, points 2–3).

C3 Evidence preservation and data minimisation.

Article 5(1)(c) of the GDPR requires personal data to be adequate, relevant and limited to what is necessary for the purposes for which they are processed (Regulation 2016/679, Art. 5(1)(c)). The Patient Data Act creates a distinct healthcare record preservation constraint. Chapter 3, Section 14 provides that information in a patient-record document may not be erased or made illegible except in the case specified by the Act, and Chapter 3, Section 17 requires a patient-record document to be retained for at least ten years after the last entry (SFS 2008:355, 3 kap. 14 §, 17 §). These provisions concern patient records rather than a general duty to retain all potential forensic evidence. For CRA-covered products, Annex I, Part I, point 2(g) separately requires data processed by the product to be adequate, relevant and limited to what is necessary for its intended purpose (Regulation 2024/2847, Annex I, Part I, point 2(g)). The analytical requirement therefore captures the tension between preserving records or evidence needed for later scrutiny and limiting the personal data processed to what is necessary.

Accountability

Accountability concerns the ability to demonstrate compliance and to attribute relevant actions to identified actors or systems. GDPR Article 5(2) makes the controller responsible for, and requires the controller to be able to demonstrate, compliance with the principles in Article 5(1) (Regulation 2016/679,

Art. 5(2)). In healthcare, this general principle is made operational through sector-specific access logging and traceability rules.

A1 Logging and monitoring.

Chapter 4, Section 3 of the Patient Data Act requires a healthcare provider to ensure that access to patient data processed wholly or partly by automated means is documented and can be checked. The same provision requires systematic and recurring checks of whether anyone has obtained unauthorised access (SFS 2008:355, 4 kap. 3 §). HSLF-FS 2016:40 makes these duties more specific. Chapter 4, Section 9 requires every user's access to patient information to be logged. Chapter 4, Section 9 a specifies that the logs show the actions taken, organisational source of access, time of access, and the identities of the user and patient. Chapter 4, Section 9 b requires systematic recurring sample checks, checks when unauthorised access is suspected, documentation of log reviews, and retention of logs for at least five years (HSLF-FS 2016:40, 4 kap. 9 §, 9 a §, 9 b §). For products within the CRA's scope, Annex I, Part I, point 2(l) requires security-related information through recording and monitoring relevant internal activity, including access to or modification of data, services or functions, with an opt-out mechanism for the user (Regulation 2024/2847, Annex I, Part I, point 2(l)).

A2 Responsibility and governance.

Article 20(1) of NIS 2 requires member states to ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken to comply with Article 21, oversee their implementation and can be held liable for infringements by the entity of Article 21, subject to the national-law qualification stated in the same provision (Directive 2022/2555, Art. 20(1)). This provides the principal governance basis for the responsibility criterion used in the analysis.

A3 Traceability and identification.

Traceability in Swedish healthcare follows directly from the access-log rules. Chapter 4, Section 9 a of HSLF-FS 2016:40 requires logs to show, among other things, the time of access and the identities of both the user and the patient. Chapter 4, Section 3 of the Patient Data Act requires access to be documented in a form that can be checked (SFS 2008:355, 4 kap. 3 §; HSLF-FS 2016:40, 4 kap. 9 a §). The EHDS Regulation similarly provides that, when the relevant provisions apply under Article 105, an electronic health record is to identify the health professional and healthcare provider that registered or updated personal electronic health data, together with the time of the action (Regulation 2025/327, Arts. 13(4), 105). For CRA-covered products, Article 13(15) requires a type, batch or serial number, or another element allowing the product to be identified (Regulation 2024/2847, Art. 13(15)). These provisions support the study's criterion that relevant actions and technical components should be traceable to identifiable actors or products.

Cyber Resilience

Cyber resilience is the capacity to prepare for, withstand, respond to and recover from disruption while maintaining essential functions (Linkov & Kott, 2018). Healthcare information systems are frequent targets of cyberattacks. The European Union Agency for Cybersecurity reports ransomware as the most common incident type affecting the European healthcare sector, with patient data being the most frequently targeted asset (ENISA, 2023). This pattern is also reflected in industry incident reporting (Verizon, 2024). Kruse et al. (2017) identify the specific consequence for healthcare: the availability of clinical systems is directly connected to patient safety, meaning that disruption carries clinical as well as financial consequences.

Three cyber resilience requirements are derived for this study.

CR1 Risk management.

Article 21(1) of NIS 2 requires member states to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage risks to the security of network and information systems used for their operations or services and to prevent or minimise the impact of incidents. Article 21(2)(a) includes policies on risk analysis and information-system security among the minimum measures (Directive 2022/2555, Art. 21(1), (2)(a)).

CR2 Operational continuity and preparedness.

Article 21(2)(c) of NIS 2 includes business continuity, such as backup management and disaster recovery, and crisis management among the minimum cybersecurity risk-management measures (Directive 2022/2555, Art. 21(2)(c)). GDPR Article 32(1)(b)–(c) also identifies, as appropriate security measures, the ability to ensure ongoing availability and resilience of processing systems and services and to restore availability and access to personal data in a timely manner after a physical or technical incident (Regulation 2016/679, Art. 32(1)(b)-(c)). In healthcare, continuity carries particular weight because the availability of clinical systems is directly connected to patient safety (Kruse et al., 2017).

CR3 Incident response and recovery.

Article 21(2)(b) of NIS 2 includes incident handling among the minimum risk-management measures. The Directive defines incident handling in Article 6(8) as actions and procedures aimed at preventing, detecting, analysing and containing incidents, or responding to and recovering from them (Directive 2022/2555, Arts. 6(8), 21(2)(b)). Article 23 adds staged reporting duties for significant incidents. Separately, GDPR Article 33(1) requires notification of a personal data breach to the competent supervisory authority without undue delay and, where feasible, within 72 hours, unless the breach is unlikely to result in a risk to natural persons' rights and freedoms (Regulation 2016/679, Art. 33(1)). Reporting is therefore treated as a related compliance obligation, while response and recovery are grounded in the NIS 2 incident-handling requirement. The nine requirements and their principal legal sources are summarised in Table 1.

Table 1
Healthcare-sector requirements and principal legal sources

Code	Requirement	Dimension	Principal source
C1	Data protection and privacy	Compliance	GDPR Arts. 5(1)(f), 9; SFS 2008:355, 1 kap. 2 §; EHDS Arts. 8, 105
C2	Interoperability and technical standards	Compliance	EHDS Art. 15(1), (4), 105; Art. 30(1)(a); Annex II, points 2–3
C3	Evidence preservation and data minimisation	Compliance	GDPR Art. 5(1)(c); SFS 2008:355, 3 kap. 14 §, 17 §; CRA Annex I, Part I, point 2(g)
A1	Logging and monitoring	Accountability	SFS 2008:355, 4 kap. 3 §; HSLF-FS 2016:40, 4 kap. 9 §, 9 a §, 9 b §; CRA Annex I, Part I, point 2(l)
A2	Responsibility and governance	Accountability	GDPR Art. 5(2); NIS 2 Art. 20(1)
A3	Traceability and identification	Accountability	SFS 2008:355, 4 kap. 3 §; HSLF-FS 2016:40, 4 kap. 9 a §; EHDS Arts. 13(4), 105; CRA Art. 13(15)
CR1	Risk management	Cyber resilience	NIS 2 Art. 21(1), (2)(a)
CR2	Operational continuity and preparedness	Cyber resilience	NIS 2 Art. 21(2)(c); GDPR Art. 32(1)(b)–(c)
CR3	Incident response and recovery	Cyber resilience	NIS 2 Arts. 6(8), 21(2)(b), 23; GDPR Art. 33(1)

2.2 Research background

This section presents the digital forensic readiness models and frameworks proposed in the research literature. The presentation is organised by type of approach, since approaches of the same type share assumptions about what forensic readiness consists of.

2.2.1 Foundational Digital Forensic Readiness Models

Foundational research on forensic readiness emphasises a structured process for preparing an organisation to collect and preserve evidence before an incident occurs. An example is Rowlingson's (2004) ten-step process, which moves from defining the business scenarios that require digital evidence and determining collection requirements to establishing policies for the secure storage and handling of evidence, ensuring that monitoring is targeted at detecting and deterring major incidents, specifying the circumstances under which escalation to a formal investigation should occur, training staff in incident awareness, documenting an evidence-based case, and ensuring legal review.

Rowlingson (2004) makes two scoping decisions that shape much of the later literature. Preventive and recovery measures are excluded from the definition of forensic readiness, which is instead defined by

what makes evidence available. A risk assessment is assumed to have already been performed, with appropriate defensive measures assumed to be in place in accordance with it. Both assumptions place risk management and recovery outside the readiness capability, positioning forensic readiness as a capability that draws on neighbouring security functions rather than containing them.

Alongside the process models, the international standard ISO/IEC 27043:2015, Information technology — Security techniques — Incident investigation principles and processes, provides guidelines for incident investigation and sets out readiness process groups describing how an organisation can become forensically ready for digital forensic investigations (Kebande & Venter, 2019). The standard also defines concurrent processes intended to run alongside investigative processes, with the purpose of assuring the admissibility of digital evidence-handling techniques throughout the investigation (Kebande & Venter, 2019). It is the most frequently referenced standard in the subsequent literature. It structures the framework developed by Kebande et al. (2020), serves as a requirements basis for Mpungu et al. (2024) and the guideline basis for Alnajjar et al. (2026), is identified as a compliance target by Fagbola and Venter (2022), and forms part of the foundation of the approach taken by Daubner et al. (2023a).

2.2.2 Existing Literature

A substantial part of the literature addresses forensic readiness as an organisational and managerial capability. Reddy and Venter (2013) propose an architecture for a digital forensic readiness management system comprising an event analysis module, an information management module for storing organisational policies and the organisational hierarchy, a costing module, and an access control module designed on the assumption that not all users of the readiness system may be trusted. The architecture requires digital forensic and incident response teams to be constituted in advance of an incident rather than after one.

Later studies building on this foundation introduced more structured frameworks that integrate technical, organisational and legal aspects of forensic readiness (Elyas et al., 2015). Elyas et al. (2015) distinguish readiness objectives—regulatory compliance, legal evidence management, forensic response and internal investigations—from the capability factors that deliver them, including organisational factors, forensic strategy, stakeholders, infrastructure, policy and training. The framework is notable for a decision that the authors explicitly report: although all focus group participants agreed that active monitoring is crucial for forensics, it was removed as a major factor because it was largely perceived as a security function. The authors state that the monitoring function is instead distributed across the other components.

Adel (2022) revises this framework for the Industry 5.0 context, elevating regulatory compliance to a high priority and reconstructing the organisational factors to include forensic control, forensic top-management level and forensic culture, while retaining the removal of monitoring. Adel et al. (2024) propose ETHICore, which establishes eight investigative positions with defined obligations and specifies privacy-enhancing technologies to minimise the exposure of personal data that is not relevant to an investigation.

Models for specific technical environments. A second strand develops readiness for particular environments where general organisational models are considered insufficient. Kebande and Venter (2019) propose a cloud forensic readiness-as-a-service model that uses a modified non-malicious botnet as a forensic agent to collect evidence without modifying the cloud infrastructure. Koen and Venter (2024) propose a federated model for applications spanning multiple provider boundaries, with a dedicated anonymisation layer so that investigations proceed on anonymised data by default, and a retention layer bounded by legal permission.

Albugmi (2024) proposes a ten-component framework for database systems covering risk assessment, data classification, encryption, database firewalls, password policies, monitoring and logging, backup

and recovery, incident response plans, forensic readiness, and education and awareness. Sulaiman et al. (2026) address Platform-as-a-Service (PaaS) cloud databases, where provider-managed log rotation can destroy evidence before an investigation begins. Jiménez et al. (2024) propose an architecture for software-defined networks with five defined stakeholder types and a constraint that infrastructure and security stakeholders cannot autonomously manipulate the record of technical actions.

Daubner et al. (2023a) propose a forensic-ready extension of information systems security risk management, in which readiness requirements are derived from identified risks. Daubner et al. (2023b) develop a reference model of the qualitative factors characterising forensic-ready software systems, including a Minimality factor that limits evidence collection to what the expected investigation requires. Kebande et al. (2020) present a holistic framework for IoT-enabled organisations built on ISO/IEC 27043, replacing the standard's abstract planning and implementation process groups with organisational, readiness and IoT security process layers. Fagbola and Venter (2022) address shadow IoT devices, which are devices connected without the knowledge of the organisation's IT function, through a six-stage model. Rahman et al. (2014) propose a forensic readiness architecture for wireless body area networks in hospitals, derived from a practical impact assessment of four wireless security threats conducted in a real-world environment.

Maturity and assessment approaches. A third strand addresses the measurement of readiness rather than its design. Englbrecht et al. (2020) propose a capability maturity model combining the characteristics of forensic readiness with the seven enablers of the COBIT 5 governance framework. The model defines five maturity levels and identifies level three as the minimum for an organisation to be considered forensically ready. Baiquni and Amiruddin (2022) apply the Digital Forensic Readiness Index, which evaluates readiness across strategy, policy and procedure, technology and security, digital forensic response, control and legality.

Comparative analyses. Comparative work on forensic readiness models is limited. Kebande and Venter (2019) note that, at the time of their study, little research had compared readiness models specifically. Their comparative analysis maps thirteen models against a cloud readiness baseline. The models target environments including small and medium enterprises, corporate environments, wireless sensor networks, wireless local area networks, cloud and mobile cloud. Most accumulate a specified type of evidence without addressing what is done with the potential evidence afterwards. The comparison is conducted against a technical baseline rather than externally defined requirements, and none of the thirteen models addresses healthcare.

A further perspective is provided by Pisarenco and Pisarenco (2026), who examine forensic infrastructure for investigating medical crimes and propose a four-level model spanning technical, procedural, institutional and legal levels. Their orientation is toward the investigation of incidents after they occur rather than proactive readiness, but the work illustrates that the forensic requirements of healthcare have also been recognised outside the computing literature.

3 Problem formulation

Healthcare organisations are required to protect special-category personal data, demonstrate who has accessed patient records, and maintain the continuity of services on which patient safety depends. These obligations were established in Section 2.1.4. Digital forensic readiness has been proposed as a proactive approach that can support all three by enabling the systematic collection, preservation and analysis of digital evidence (Rowlingson, 2004; Kebande et al., 2020). Section 2.2 presented the models and frameworks proposed in the research literature. What has not been established is how well these approaches correspond to the obligations that actually apply.

The gap this study addresses concerns the application and evaluation of DFR models and frameworks within healthcare specifically, rather than a general absence of analysis. The models presented in Section 2.2 are primarily developed for general organisational or technical environments; where a sector-specific context appears, it is typically treated as an application context rather than as a source of design requirements. Existing comparative work compares models against one another on technical grounds. Kebande and Venter (2019), for example, compare thirteen models based on process overlap without considering whether they satisfy regulatory requirements, and none of the thirteen addresses healthcare.

Healthcare introduces two conditions that make this comparison necessary. First, health data are classified as special-category personal data under Article 9 of the GDPR, and healthcare-specific instruments apply in addition to cross-sectoral ones. The EHDS Regulation and, in Sweden, the Patient Data Act (Patientdatalag) and its supporting regulations impose requirements including access verification that have no direct equivalent in most sectors (SFS 2008:355; HSLF-FS 2016:40).

Second, the consequences of unavailability differ in kind. In other critical infrastructure sectors, service interruption causes economic and social harm. In healthcare, the availability of clinical systems is connected to patient safety (Kruse et al., 2017), meaning that a forensic readiness capability that impairs system operation carries a cost that no evidential benefit offsets.

These conditions mean that general organisational readiness models cannot be assumed to transfer to healthcare without examination. A structured comparison against healthcare requirements is therefore needed to establish which requirements existing approaches support and where gaps remain.

3.1 Study aims

This study aims to compare existing digital forensic readiness models and frameworks against the compliance, accountability and cyber resilience requirements that apply to the Swedish healthcare sector, and to identify where those requirements are not supported. It seeks to bridge the gap between theoretical forensic readiness frameworks and their practical governance implications in healthcare cybersecurity.

The study does not develop a new model. Its contribution is a structured and traceable mapping that makes both coverage and gaps explicit.

3.2 Research Question and Guidance Questions

The research question is "Which requirements related to compliance, accountability and cyber resilience within the Swedish healthcare sector are supported by existing Digital Forensic Readiness (DFR) models and frameworks, and which gaps remain?"

Three guidance questions structure the work. The healthcare-sector requirements are established in Section 2.1.4 and are not identified as part of the analysis. The guidance questions are:

1. What criteria are used to select DFR models and frameworks for the comparative analysis?
2. How are the requirements presented in Section 2.1.4 operationalised into an analytical framework for comparing the selected models and frameworks?
3. To what extent do existing DFR models and frameworks support the healthcare-sector requirements related to compliance, accountability and cyber resilience, and which gaps remain?

The research question is descriptive and comparative. It seeks to characterise and compare existing approaches rather than design a new one, and its findings are bounded by the Swedish and European Union regulatory context.

3.3 Motivation

The motivation for this study is both academic and practical. From a research perspective, digital forensic readiness has undergone significant development since it was first formulated as proactive evidence preservation. Later work has extended the concept to maturity assessment (Bankole et al., 2022), federated cloud evidence management (Koen & Venter, 2024), ethical oversight (Adel et al., 2024), insider risk monitoring (Daubner et al., 2023a), and forensic-by-design integration in medical systems (Grispos et al., 2017). These approaches were developed for different environments and with different assumptions about what readiness consists of, and studies tend to examine a specific technical challenge or an isolated governance concern. The three dimensions considered here are rarely examined together, which means their combined contribution to a regulated sector remains unclear.

Each dimension matters for a distinct reason. Compliance is essential because healthcare organisations process special-category personal data under strict obligations to secure it and to report breaches within defined time frames, with substantial administrative fines possible for non-compliance (Regulation 2016/679; Directive 2022/2555). Accountability is critical because healthcare systems must be able to trace user actions and maintain reliable audit trails, so that incidents can be investigated, responsible parties can be identified, and evidence can be used in legal and regulatory contexts (Rowlingson, 2004). Cyber resilience is vital because disruption affects patient safety directly: organisations must be able to detect, respond to and recover from incidents while maintaining continuous operation (Linkov & Kott, 2018). Ransomware attacks on healthcare have demonstrated how cybersecurity failures translate into consequences for patient safety and operational continuity (Shahzadi et al., 2025).

From a practical perspective, decision makers require structured guidance on selecting and implementing forensic readiness approaches that preserve evidence while also strengthening governance and resilience. A healthcare organisation choosing between the reviewed approaches has no basis within this literature for determining which of its obligations each one supports.

The relevance to network and system administration (NSA) follows from the technical functions examined in the review. The included approaches rely on centralised logging, network monitoring, authentication

and access control, evidence retention, backup and recovery, and incident response mechanisms implemented within networked and server-based infrastructure. The study therefore concerns how healthcare systems can be administered so that relevant evidential records remain available, attributable and protected while essential services continue to operate. In this sense, the compliance, accountability and cyber resilience requirements examined here are directly connected to the configuration and operation of networks, servers, logging services and recovery mechanisms.

The study therefore has both theoretical and practical relevance. Theoretically, it synthesises existing forensic readiness approaches within a governance framework derived from the obligations applying to healthcare. Practically, it shows healthcare organisations which compliance, accountability and cyber resilience requirements the reviewed literature supports, and where gaps remain.

3.4 Delimitations

The study is literature-based and includes no primary empirical data collection. No interviews, surveys, case studies or experiments were conducted, and no model was implemented or tested in an operational environment. The findings describe what the reviewed literature establishes about these models, not how they perform in practice.

The analysis is restricted to compliance, accountability and cyber resilience. Cost, usability, performance, scalability and organisational culture are outside the scope. The regulatory scope is Swedish and European. Requirements arising under other jurisdictions are not considered, and the findings should not be assumed to transfer to healthcare systems governed by different instruments without further analysis.

The models examined are drawn from peer-reviewed academic literature. Sources in English and Swedish were considered, while literature published in other languages was excluded.

4 Methodology

This study examines existing digital forensic readiness models and frameworks in relation to compliance, accountability and cyber resilience requirements within the healthcare sector. Answering this question requires qualitative information of a specific kind: descriptions of the models themselves, the components and processes they specify, and the environments they address.

Several alternatives were considered. Interviews or surveys would have provided primary data on how forensic readiness is understood and practised in Swedish healthcare organisations. They were not selected for two reasons. The research question concerns the properties of published models rather than those of any organisation's practice, so practitioner accounts would answer a different question. Recruiting participants with relevant expertise, obtaining ethical approval for data collection concerning security practices in a sensitive sector, and completing the analysis were also judged unlikely to fit the time frame. A case study in a single healthcare organisation would have allowed detailed examination of readiness in an operational setting, but a single case cannot support the comparative element of the research question, which requires the models themselves to serve as the units of analysis.

Among literature-based methods, Paré and Kitsiou (2017) distinguish several review types with different objectives. A narrative review interprets prior knowledge qualitatively but follows an unstructured approach to selecting the literature it discusses, which would not produce a traceable account of how models were located and selected. A descriptive or mapping review determines the extent to which a body of literature reveals interpretable patterns, typically concerning publication trends; the research question here is not about the shape of the research landscape. A scoping review provides an initial indication of the size and nature of a body of literature and is often used to determine whether a full systematic review is warranted, making it a preliminary rather than a final review approach for this study.

Based on the nature of the research question and the available evidence, a Structured Literature Review (SLR) was selected as the most suitable method for systematically identifying, analysing and comparing relevant studies. Paré and Kitsiou (2017) characterise this form of review as answering a clearly formulated question through a documented search, predefined eligibility criteria and systematic extraction from the selected studies. This matches the structure of the research question, which requires a defensible set of models to compare and a consistent basis for comparing them. It also permits the analysis to be audited because the selection criteria and extraction procedure are defined in advance, allowing another researcher to examine how each conclusion was reached.

The review follows the six generic steps described by Paré and Kitsiou (2017):

1. Formulate a research question or aim
2. Perform literature searches
3. Apply inclusion and exclusion criteria
4. Perform quality assessment
5. Extract data
6. Analyse data

Step 1 is addressed in Chapter 3. Steps 2 to 4 are described in Section 4.1 (Data Collection), and Steps 5 and 6 in Section 4.2 (Data Analysis). Paré and Kitsiou (2017) also distinguish three coverage strategies: exhaustive coverage, coverage representative of a field, and coverage concentrating on pivotal works. This study adopts representative coverage for the models in Chapter 2, which establish the broader

forensic-readiness context, and exhaustive coverage within a defined scope for the studies included in the review, for which records from a documented search across seven databases were screened against predefined criteria.

4.1 Data collection

This subsection describes the source-retrieval routes, database search, eligibility criteria, screening process and study selection.

4.1.1 Two Retrieval Routes

Two distinct types of sources were required, and they were retrieved differently. Peer-reviewed literature describing DFR models and frameworks was retrieved through systematic searching of academic databases, as described below.

The legal and regulatory instruments from which the requirements in Section 2.1.4 were derived were not sourced from academic databases. Laws, regulations and directives are not indexed there, and searching for them in that way would not be an appropriate retrieval strategy. The six instruments—the GDPR, the NIS 2 Directive, the Cyber Resilience Act, the EHDS Regulation, the Patient Data Act (Patientdatalag), and HSLF-FS 2016:40—were obtained from official sources: the consolidated legislative texts published by the European Union on EUR-Lex, the consolidated text published by the Swedish Riksdag, and the regulations published by the Swedish National Board of Health and Welfare. The role of the academic literature in relation to the requirements was limited to identifying which instruments are treated as relevant to healthcare cybersecurity; the authoritative wording of each requirement was taken from the legislative source itself. This distinction is stated explicitly because the two routes differ in kind and should not be conflated.

4.1.2 Database and Search String

Academic literature was searched systematically across seven databases: IEEE Xplore, Web of Science, Scopus, Springer Nature Link, ScienceDirect, ACM Digital Library and Europe PMC. The database searches were conducted between February and August 2026. These databases were selected because of their relevance and credibility in the fields of computing, information systems and health informatics. The search string used across the databases was as follows:

("Digital forensics" OR "Incident response plans" OR "Playbooks for Incident Response" OR "digital forensic readiness model" OR "digital forensic readiness framework" OR "digital forensic readiness approach")

AND

(healthcare OR hospital OR health sector)

Europe PMC was included so that a health-oriented database would be searched, since forensic readiness work situated in health informatics may not be indexed in the computing databases. A PubMed search was attempted first but returned a message indicating that four of the quoted phrases were not present in its phrase index; Europe PMC was therefore used instead.

The string was adapted to each platform because databases differ in field codes, phrase-search support and Boolean operator limits. ScienceDirect permits a maximum of eight Boolean connectors per field, which the string satisfies exactly, and Springer Nature Link provides no field-restricted search other than by title.

4.1.3 Inclusion and Exclusion Criteria

The inclusion and exclusion criteria are given in Table 2. They distinguish peer-reviewed academic literature retrieved from databases from regulatory and standards documents retrieved from official sources.

Table 2
Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Peer-reviewed journal articles, conference papers, or reviews.	Non-peer-reviewed publications.
Published in English or Swedish.	Publications without full-text availability.
Full-text availability.	Studies not written in English or Swedish.
Addresses digital forensic readiness or proactive forensic readiness.	Studies focused only on post-incident digital forensics without a forensic readiness component.
Presents a model, framework, or structured approach.	Studies that do not present a model, framework, or structured approach.
Relevant to healthcare, hospitals, medical systems, or healthcare-related environments.	Studies with no relevance to healthcare or healthcare-related environments.
Provides sufficient detail to assess the approach against the study's requirements.	Studies that provide insufficient detail for analysis.
No publication date restriction.	Duplicate publications.

No publication date limit was applied. Foundational forensic readiness work remains directly relevant to current models, as Section 2.2.1 sets out, and applying a date limit would have excluded the original definition on which the field is built.

4.1.4 Screening

Screening followed Step 3 of the review process. The titles and abstracts of the identified studies were reviewed first, and records clearly failing one or more exclusion criteria were removed at this stage. The remaining records were retrieved in full text and assessed against the complete set of criteria.

Step 4 was used as a minimum quality and eligibility threshold rather than as a formal methodological quality score. Publications had to be peer reviewed, retrievable in full text, and sufficiently specific to permit evidence extraction against the predefined requirements. A study satisfying the topical criteria but describing its approach too abstractly to allow evidence extraction was recorded as excluded, with that reason stated, rather than included and coded as providing no evidence. This distinction matters for interpretation: an exclusion on the grounds of insufficient specification is a statement about the reviewed text, not about the methodological quality or potential capability of the model it describes.

4.1.5 Study Selection

The search identified 1,868 records across seven databases after the platform-specific filters had been applied. After 263 duplicate records were removed, a further 568 records were identified as not relevant

to the topic and removed before formal title-and-abstract screening. The titles lacked relevance to the research topic, and they were therefore removed. The remaining 1,037 records entered title-and-abstract screening. A total of 882 records were excluded at that stage. Full text was sought for the remaining 155 records. A total of 58 reports were retrieved and assessed against the complete eligibility criteria, while 97 could not be retrieved in full text and therefore did not satisfy the full-text availability criterion. Of the 58 reports assessed for eligibility, 43 were excluded, leaving 15 studies in the review. The selection process is summarised in Figure 1.

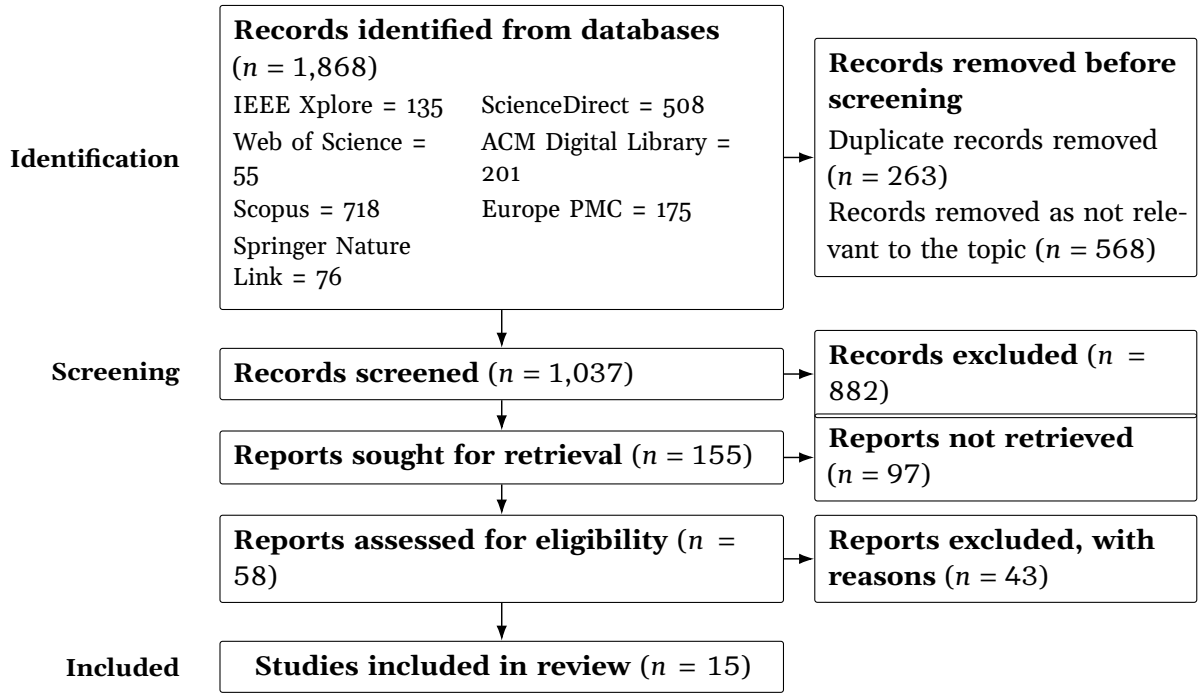

Figure 1
Study selection process

4.2 Data analysis

This section describes Step 5 (extracting data) and Step 6 (analysing data).

4.2.1 Analytical Approach

The included studies were analysed using thematic analysis as described by Braun and Clarke (2006). A deductive approach was taken; the themes were defined in advance from the requirements in Section 2.1.4 rather than derived from the studies. This is appropriate because the analysis asks whether a predetermined set of requirements is addressed, which presupposes that the requirements are fixed before the studies are read.

Three primary themes were used, corresponding to the three dimensions in the research question. Within each, three sub-themes were defined, following the principle that sub-coding permits a more detailed and nuanced interpretation than coding at the level of the primary theme alone (Saldaña, 2013, pp. 279–282).

For compliance, the sub-themes were data protection and privacy, interoperability and technical standards, and evidence preservation and data minimisation. For accountability, the sub-themes were logging and monitoring, responsibility and governance, and traceability and identification. For cyber resilience,

the sub-themes were risk management, operational continuity and preparedness, and incident response and recovery.

4.2.2 Data Extraction

Data extraction was performed on the full text of each included study. For each study, the following were recorded: the stated purpose and objective, the environment addressed, the name and type of the approach, its principal components, the method by which it was developed or evaluated, its stated limitations, and any content bearing on the nine sub-themes.

Each extracted item was recorded together with the section or page in which it appeared, so that every coding decision can be traced to a specific location in a specific source. The evidence used for the coding decisions is given in Appendix B.

4.2.3 Coding Framework

The comparison uses four codes, defined before coding began, as presented in Table 3.

Table 3
Coding framework

Code	Definition
D – Direct evidence	The study explicitly describes a mechanism, component or process corresponding to the sub-theme and identifies it as part of the proposed approach.
I – Indirect evidence	The study describes something that plausibly contributes to the sub-theme but does not address it explicitly, or states it as a general aim without specifying how the approach realises it.
NE – Not evidenced	The study was read in full for the sub-theme and contains no content bearing on it. This is a statement about the reviewed text, not about the approach's capabilities.
U – Unclear	The study contains content that may bear on the sub-theme but is too ambiguous or underspecified to support a reliable decision.

Two general boundary rules were applied uniformly. The D/I boundary turns on whether the requirement is addressed as an identifiable element of the approach—a named component, layer, stage, process, or indicator—or is only implied by something else the approach does. The I/NE boundary turns on whether any content in the study bears on the requirement at all.

To reduce the subjectivity of these boundaries, a decision rule was written for each of the nine sub-themes before coding began, specifying what counts as direct and what counts as indirect in that specific case. The coding framework is summarised in Table 3, and the evidence trail documenting how the rules were applied to each coding decision is provided in Appendix B.

Two limits on interpretation were applied throughout. First, a coded capability is not a finding of legal compliance, meaning that a study describing logging provides evidence of a logging capability, not evidence that a system implementing the approach would satisfy the access-verification obligation in Chapter 4, Section 3 of the Swedish Patient Data Act (SFS 2008:355). This depends on how the capability is configured and operated in a specific deployment. Second, a code of NE records that the reviewed publication does not evidence a requirement, not that the approach could not support it.

4.2.4 Synthesis

Following coding, the studies were compared across the nine sub-themes to identify patterns in coverage, differences between approaches designed for different environments, and requirements addressed by few or none. The synthesis is organised by requirement rather than by study, so that the analysis reports what the body of included literature collectively addresses rather than summarising each study in turn.

4.3 Validity and Reliability

Ensuring validity and reliability is essential for establishing the credibility of a qualitative study. In this research, several steps were taken to ensure that the findings are both trustworthy and consistent (Berndtsson et al., 2008).

To ensure validity, a systematic and transparent literature selection process was applied. The use of predefined inclusion and exclusion criteria helped ensure that studies relevant to the research question were included in the analysis. This is important for reducing bias during study selection, since the search strategy must balance the identification of relevant primary studies with the exclusion of irrelevant papers (Wohlin et al., 2012). Additionally, the research process was closely aligned with the research question, ensuring that the study addressed its intended purpose. The use of thematic analysis with predefined themes (compliance, accountability and cyber resilience) further strengthened validity by grounding the analysis in the research objectives rather than allowing the analytical categories to be driven solely by subjective interpretation.

To ensure reliability, the study followed a consistent methodological strategy throughout the research process. The search terms, databases and selection criteria were applied systematically. The coding process was also conducted using a structured framework, providing consistency in how data were analysed across the included studies. Any deviations from the initial research strategy were carefully considered and documented. A limitation of the analysis is that the screening, data extraction and coding were conducted by a single researcher. Although predefined coding values were used to distinguish between direct, indirect, not evidenced, and unclear evidence, some interpretive judgement was still required when classifying borderline cases. This may affect the consistency of individual coding decisions. To reduce risk, the same coding framework and decision rules were applied across all included studies, and each coding decision was linked to a specific passage in the reviewed article. The complete evidence trail is provided in Appendix B, allowing the coding decision to be examined and assessed by the reader.

4.4 Ethical Aspects

The study is based on published secondary sources and involves no human participants, so questions of informed consent and participant confidentiality do not arise directly. All sources are cited and referenced in accordance with academic practice.

The subject matter nonetheless raises ethical considerations bearing on the interpretation of the findings. Forensic readiness rests on monitoring and logging, and in a healthcare setting these record the activity of clinical staff and, indirectly, information about patients. A capability that improves an organisation's ability to investigate incidents also increases its capacity to observe its own personnel. Article 5(1)(c) of the GDPR requires that processing be limited to what is necessary for the purpose (Regulation 2016/679, Art. 5(1)(c)), and the Swedish Patient Data Act requires healthcare information management to respect the privacy of patients and other data subjects (SFS 2008:355, 1 kap. 2 §). These considerations are discussed in relation to the results in Section 6.2.

This study analyses only published descriptions of models and frameworks. No personal data were processed during the research itself.

5 Results

This chapter presents the results of the structured literature review and answers the research question "Which requirements related to compliance, accountability and cyber resilience within the Swedish healthcare sector are supported by existing Digital Forensic Readiness (DFR) models and frameworks, and which gaps remain?" Section 5.1 describes the characteristics of the included studies. Sections 5.2 to 5.4 report the evidence for compliance, accountability and cyber resilience requirements, respectively. Section 5.5 compares the healthcare-specific literature with the general forensic readiness literature presented in Chapter 2. Section 5.6 synthesises the findings across studies and identifies the remaining gaps.

Throughout this chapter, a coded capability is reported as evidence of what an approach specifies, not as a finding that a system implementing it would satisfy a legal obligation. Where a reviewed study asserts compliance, that assertion is reported as the study's own claim.

5.1 Characteristics of the Included Studies

The fifteen included studies were published between 2012 and 2026 and address a range of healthcare and healthcare-relevant environments. Their characteristics are summarised in Table 4, with the abbreviation S used for the study IDs.

Table 4
Characteristics of the included studies

ID	Study	Environment	Approach	Method
S1	Chernyshev et al. (2019)	Electronic medical records	Forensic audit logging architecture	Conceptual; comparison of six EMR systems
S2	Grispos et al. (2017)	Medical cyber-physical systems	Forensic-by-design framework, nine components	Conceptual; hypothetical case study
S3	Yaqub et al. (2026)	Point-of-care ultrasound	URSA volatile-first readiness workflow	Empirical; seven memory acquisitions
S4	Mpungu et al. (2024)	Wireless medical networks	Secure decentralised Big Data framework	Framework design; scenario evaluation
S5	Mishra & Bagade (2022)	Medical Internet of Things	Forensic-ready MIoT methodology	Framework design; ML intrusion detection
S6	Al-Balasmeh (2026)	Medical IoT	Edge framework with permissioned blockchain	Prototype; 50-device testbed
S7	Zehra et al. (2024)	Blockchain electronic health records	Testbed-based auditing and forensics process	Experimental; three-node blockchain
S8	Kyaw et al. (2019)	Wireless medical systems	Eight-component DFR framework	Conceptual; expert evaluation
S9	Kyaw et al. (2020)	Wireless medical systems	Extended DFR framework	Design science; expert evaluation
S10	Cusack & Kyaw (2012)	Hospital wireless networks	Forensically ready network architecture	Conceptual proposal
S11	Gombar et al. (2026)	Critical infrastructure	FROM operational model, four pillars	Survey; PLS-SEM, 212 respondents
S12	Mekala et al. (2025)	Industrial IoT	Seven-stage framework, Purdue-aligned	Framework design; testbed evaluation
S13	Adel et al. (2024)	Organisational	ETHICore compliance and oversight framework	Literature review; focus groups
S14	Bankole et al. (2022)	Organisational	Extended readiness and maturity model	Comparative analysis; 10 interviews
S15	Janjua et al. (2020)	Fog-enabled cloud IoT	PLAF log-preservation architecture	Architecture design; implemented testbed

Ten studies address healthcare directly (S1–S10). Five address environments materially relevant to healthcare while naming healthcare within the reviewed text (S11–S15).

Three studies form a research lineage. Cusack and Kyaw (2012), Kyaw et al. (2019) and Kyaw et al. (2020) report successive stages of one programme on wireless medical systems, each elaborating on the previous design. They are treated as three studies because each reports a distinct design at a different level of specification, but their agreement reflects developmental continuity rather than independent replication, and this is taken into account in the synthesis.

The studies differ in how far their proposals have been evaluated. Five report empirical evaluation of their approaches on real or simulated systems (S3, S6, S11, S12, S15). Two apply the approach to a documented case or scenario (S4, S7). Three report expert evaluation (S8, S9, S14). Five are conceptual and not evaluated (S1, S2, S5, S10, S13).

No included study reports implementation of the approach in an operational healthcare setting. Yaqub et al. (2026) come closest, acquiring memory from genuine clinical ultrasound hardware, but state that this was done in a controlled setting and not during patient care. Several studies state this limitation themselves: Mpungu et al. (2024) identify prototype development as future work, and Kyaw et al. (2019) report that expert reviewers recommended implementation and testing in a controlled laboratory environment to validate the conceptual design. The results in this chapter therefore describe what these approaches specify, not what they achieve when deployed.

5.2 Compliance Requirements

The evidence for the three compliance requirements is presented in Table 5.

Table 5
Evidence for compliance requirements

ID	Study	C1 Data protection and privacy	C2 Interoperability and standards	C3 Preservation and data minimisation
S1	Chernyshev et al. (2019)	I	D	D
S2	Grispos et al. (2017)	D	D	D
S3	Yaqub et al. (2026)	D	I	D
S4	Mpungu et al. (2024)	D	D	D
S5	Mishra & Bagade (2022)	I	I	D
S6	Al-Balasmeh (2026)	D	D	D
S7	Zehra et al. (2024)	I	I	I
S8	Kyaw et al. (2019)	I	D	D
S9	Kyaw et al. (2020)	I	D	D
S10	Cusack & Kyaw (2012)	I	I	I
S11	Gombar et al. (2026)	D	I	D
S12	Mekala et al. (2025)	I	D	D
S13	Adel et al. (2024)	D	I	D
S14	Bankole et al. (2022)	I	D	D
S15	Janjua et al. (2020)	D	I	D
Total	Direct evidence	7 (47%)	8 (53%)	13 (87%)

5.2.1 Data Protection and Privacy

Seven of fifteen studies provide direct evidence of mechanisms protecting personal or sensitive data. The direct treatments differ in what they protect. Yaqub et al. (2026) make privacy-aware handling a named readiness objective requiring encryption, controlled access and retention limits, and apply these to the conduct of the study itself. Grispos et al. (2017) make privacy requirements one of nine framework components and explicitly identify that privacy requirements may conflict with forensic strategies rather than assuming compatibility. Mpungu et al. (2024) specify disk-level and file-level encryption, access control lists, and a Data Privacy Officer role. Al-Balasmeh (2026) keeps patient data off the blockchain specifically to preserve privacy. Janjua et al. (2020) apply homomorphic encryption so that logs can be validated without exposing their contents. Adel et al. (2024) specify privacy-enhancing technologies to minimise the exposure of personal data not relevant to an investigation. Gombar et al. (2026) make governance and privacy one of four model pillars, with indicators drawn from GDPR readiness instruments.

The eight indirect treatments share a common characteristic: they protect the network or the evidence store rather than the data subject. This is most visible in the wireless medical lineage. Cusack and Kyaw (2012) identify privacy as one of two security dimensions at risk but specify no protective mechanism.

Kyaw et al. (2019, 2020) analyse weaknesses in wireless encryption and design their frameworks to address them. They also apply integrity checking to the patient database so that changes are detected and logged, but neither approach protects the patient as a data subject. Mishra and Bagade (2022) state privacy assurance as a purpose but describe encryption as something medical devices cannot support because of resource constraints.

The distinction matters for the Swedish context. Article 9(1) of the GDPR includes data concerning health among the special categories of personal data (Regulation 2016/679, Art. 9(1)). In Sweden, the Patient Data Act requires healthcare information management to be organised so that the privacy of patients and other data subjects is respected and documented personal data is handled and stored so that unauthorised persons cannot access it (SFS 2008:355, 1 kap. 2 §). An approach that secures the network on which patient data travels and detects modification of the record does not thereby protect patients' data from unauthorised viewing.

5.2.2 Interoperability and Technical Standards

Eight studies name a standard or address interoperability directly.

ISO/IEC 27043:2015 serves as the principal reference standard. It structures the requirements identification process in Mpungu et al. (2024) and informs the definition of readiness used by Kyaw et al. (2019). Bankole et al. (2022) require that policies be implemented according to agreed standards and set laboratory accreditation to ISO 17025 as an objective. Mekala et al. (2025) build on the Purdue model for industrial control systems and incorporate ENISA guidelines, the MITRE ATT&CK framework, CVSS and CAPEC, proposing alignment with ISO/IEC 27043 as future validation.

Interoperability in the sense of systems exchanging information is addressed by fewer studies. Mpungu et al. (2024) specify multiple interfaces enabling investigators, data scientists and healthcare researchers from different organisations to access evidential data securely. Al-Balasmeh (2026) normalises heterogeneous artefact formats at the edge, addressing the problem that medical IoT devices log differently from one another. Chernyshev et al. (2019) describe their architecture as generic and implementation-agnostic, applicable across on-premise, cloud and healthcare IoT deployments.

No included study engages with a healthcare-sector interoperability standard. The EHDS Regulation makes interoperability a structural requirement for sharing electronic health data across the European Union, and Sweden is implementing a national digital infrastructure on that basis, with certain categories of health data required to be shared from March 2029 (E-hälsomyndigheten, 2025). The reviewed literature contains no approach designed against those requirements.

5.2.3 Evidence Preservation and Data Minimisation

Evidence preservation is the second most consistently supported requirement in the review, addressed directly by thirteen of the fifteen studies. The mechanisms converge across environments that otherwise share little. Cryptographic hashing appears in approaches for medical devices (Yaqub et al., 2026), wireless medical networks (Mpungu et al., 2024), and hospital wireless systems (Kyaw et al., 2019, 2020). Chain of custody is named by Chernyshev et al. (2019), Mekala et al. (2025), Al-Balasmeh (2026), and Bankole et al. (2022). Tamper-evident storage is specified by Al-Balasmeh (2026), whose framework records only hash-based integrity anchors and custody metadata on a permissioned ledger while keeping raw artefacts off-chain, and by Janjua et al. (2020), whose architecture preserves log integrity, provenance, verifiability and ownership non-repudiation. Forensically sound acquisition is specified by Mpungu et al. (2024), who attach a write blocker to ensure read-only access, and by Mishra

and Bagade (2022), who specify the memory acquisition procedure step-by-step. The two studies coded as indirect are Zehra et al. (2024), who invoke blockchain immutability as a property of the underlying platform rather than specifying a preservation mechanism of their own, and Cusack and Kyaw (2012), whose proposal forwards captured packets to a forensic server without addressing their integrity. Data minimisation is addressed far less often. Of the fifteen studies, four engage with it: Adel et al. (2024) require the exclusion of data irrelevant to an investigation from reports, on the grounds that this prevents dilution of findings and reduces the risk of privacy violations; Al-Balasmeh (2026) keeps raw artefacts off-chain, restricting what enters the immutable ledger; Mekala et al. (2025) score artefact relevance as low, medium or high against attack scenarios; and Cusack and Kyaw (2012) note that the cost of information storage is balanced against the benefit of having the evidence available. None frames the amount of personal data processed in the terms required by Article 5(1)(c) of the GDPR. Two studies state positions that run in the opposite direction. Mpungu et al. (2024) build their framework on comprehensive retention of structured, semi-structured and unstructured data. Yaqub et al. (2026) are an exception among the healthcare studies, applying data-minimisation principles to their own handling of acquired memory images.

5.3 Accountability Requirements

The evidence for the three accountability requirements is presented in Table 6.

Table 6
Evidence for accountability requirements

ID	Study	A1 Logging and monitoring	A2 Responsibility and governance	A3 Traceability and identification
S1	Chernyshev et al. (2019)	D	I	D
S2	Grispos et al. (2017)	D	D	I
S3	Yaqub et al. (2026)	D	D	D
S4	Mpungu et al. (2024)	D	D	D
S5	Mishra & Bagade (2022)	D	NE	D
S6	Al-Balasmeh (2026)	D	I	D
S7	Zehra et al. (2024)	D	I	D
S8	Kyaw et al. (2019)	D	NE	D
S9	Kyaw et al. (2020)	D	NE	D
S10	Cusack & Kyaw (2012)	D	NE	I
S11	Gombar et al. (2026)	D	D	D
S12	Mekala et al. (2025)	D	D	D
S13	Adel et al. (2024)	NE	D	I
S14	Bankole et al. (2022)	D	D	I
S15	Janjua et al. (2020)	D	I	D
Total	Direct evidence	14 (93%)	7 (47%)	11 (73%)

5.3.1 Logging and Monitoring

Logging and monitoring is the best-supported requirement in the review, addressed directly by fourteen of the fifteen studies.

In several studies, it is the foundational component. Chernyshev et al. (2019) propose an architecture whose entire function is forensic audit logging for electronic medical records. Kyaw et al. (2019, 2020) aggregate logs from eight components to a centralised server. Mpungu et al. (2024) combine security information and event management logging with behavioural analytics over decentralised storage. Al-Balasmeh (2026) performs capture at the network edge specifically because medical IoT devices cannot retain their logs long enough for later collection. Janjua et al. (2020) automate continuous log collection using non-malicious command-and-control botnets.

The single exception is Adel et al. (2024), whose framework specifies no logging mechanism at any point. This is consistent with a position taken elsewhere in the wider forensic readiness literature: Elyas et al. (2015), on whose framework the ETHICore work builds, report that monitoring was removed as a major factor on the grounds that it is perceived as a security rather than a forensic function. Section 5.5 returns to this.

A finding within this consensus concerns what is logged. Chernyshev et al. (2019) examined audit logging in six open-source electronic medical record systems and report that, while most log the creation and modification of patient records, the majority do not track viewing activity. Kyaw et al. (2020) are the only included study whose logging reaches the clinical application layer, capturing user logins, failed logins and setting changes within the OpenEMR system. Even there, what is captured is authentication and change, not access to a record.

The Swedish Patient Data Act requires care providers to ensure that automated access to patient data is documented and can be checked (SFS 2008:355, 4 kap. 3 §). HSLF-FS 2016:40 further requires systematic and recurring sample-based review of access logs and checks when unauthorised access is suspected (HSLF-FS 2016:40, 4 kap. 9 b §). The distinction between logging modifications and logging access is therefore material to the access-verification obligation.

5.3.2 Responsibility and Governance

Seven studies address responsibility and governance directly, four provide indirect evidence, and four provide none. This requirement has the highest count of not-evidenced codes in the review.

The four studies with no governance content share a characteristic: all are component-level technical designs. Cusack and Kyaw (2012), Kyaw et al. (2019), Kyaw et al. (2020), and Mishra and Bagade (2022) specify in detail what a system does, which components capture what, how integrity is verified, and how logs are aggregated, but specify nothing about who is responsible for any of it. Three of the four are designs for hospital environments.

Where governance is present, the treatments are substantial. Adel et al. (2024) establish eight investigative positions with individual obligations, from case handler through to legal prosecutor. Bankole et al. (2022) require an organisational structure depicting the forensic unit and its responsibilities, and specify separation of duties: investigations should not be approved by the same group performing them. Mpungu et al. (2024) define an incident response team by role, class and responder level, with escalation determined by incident severity. Grispos et al. (2017) require staff training in incident awareness so that all those involved understand their role in the digital evidence process. Gombar et al. (2026) make governance one of four pillars, with algorithmic accountability mechanisms as an operationalised indicator.

Article 20(1) of the NIS 2 Directive requires member states to ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken to comply with Article 21, oversee their implementation and can be held liable for infringements by the entity of Article 21, subject to the qualification in that provision (Directive 2022/2555, Art. 20(1)). Article 5(2) of the GDPR requires the controller to be responsible for and able to demonstrate compliance with the principles in Article 5(1) (Regulation 2016/679, Art. 5(2)). An approach specifying no responsible party supports neither requirement as written.

5.3.3 Traceability and Identification

Eleven studies address traceability directly. The mechanisms vary with the environment. Kyaw et al. (2019, 2020) tie actions to an authenticated username, a device MAC address and a timestamp through a RADIUS server, with a database of legitimate access points and client addresses held for comparison. Al-Balasmeh (2026) makes chain of custody cryptographically verifiable with blockchain-anchored time ordering. Mishra and Bagade (2022) recover process lineage and parent-child relationships from device memory and identify network conversations and endpoints. Janjua et al. (2020) assure ownership non-repudiation so that logs can be attributed to their originating party in a multi-stakeholder environment.

Three studies demonstrate attribution empirically in a healthcare context. Mpungu et al. (2024) trace access patterns, medication administration records and device interactions to an individual clinician in a scenario based on a documented case. Zehra et al. (2024) reconstruct impersonation of a registered doctor from blockchain transaction logs, showing that an attacker exploiting a missing access check can delete records added by a verified doctor and add falsified ones that the patient subsequently sees. Chernyshev et al. (2019) tie audit records to user and device context, the time of activity, and the categories of health information involved.

These demonstrations matter because they address a threat faced by healthcare organisations. Chernyshev et al. (2019) focus on privilege abuse on the basis that internal actors account for most healthcare breach incidents.

5.4 Cyber Resilience Requirements

The evidence for the three cyber resilience requirements is presented in Table 7.

Table 7
Evidence for cyber resilience requirements

ID	Study	CR1 Risk management	CR2 Continuity and preparedness	CR3 Incident response and recovery
S1	Chernyshev et al. (2019)	I	I	I
S2	Grispos et al. (2017)	D	D	D
S3	Yaqub et al. (2026)	I	D	I
S4	Mpungu et al. (2024)	D	D	D
S5	Mishra & Bagade (2022)	D	I	I
S6	Al-Balasmeh (2026)	NE	I	I
S7	Zehra et al. (2024)	I	NE	I
S8	Kyaw et al. (2019)	I	I	D
S9	Kyaw et al. (2020)	I	I	D
S10	Cusack & Kyaw (2012)	I	D	I
S11	Gombar et al. (2026)	I	D	D
S12	Mekala et al. (2025)	D	I	I
S13	Adel et al. (2024)	I	I	I
S14	Bankole et al. (2022)	D	NE	D
S15	Janjua et al. (2020)	NE	I	I
Total	Direct evidence	5 (33%)	5 (33%)	6 (40%)

5.4.1 Risk Management

Five of fifteen studies address risk management directly, making it one of the two weakest requirements.

Where present, it is structural. Grispos et al. (2017) make risk assessment the first of nine framework components and use it to identify the potential incidents to which forensic readiness principles are then applied. Mpungu et al. (2024) conduct a risk assessment within the requirements phase and use it to define the scenarios the framework addresses. Mekala et al. (2025) place threat and vulnerability assessment in the first of seven stages, using MITRE ATT&CK for threat intelligence and CVSS for vulnerability prioritisation. Mishra and Bagade (2022) build a medical IoT threat model on trust boundaries between the device, smartphone application and cloud, and use its output to inform the intrusion detection design. Bankole et al. (2022) describe their Systems and Events domain as essentially a risk assessment conducted at the business level.

Among the ten remaining studies, risk appears as motivating context rather than as a component. Cusack and Kyaw (2012) describe forensic readiness as a prudent risk treatment without specifying a risk process. Kyaw et al. (2019) claim the framework is suitable for security risk coverage without including a risk

component. Al-Balasmeh (2026) and Janjua et al. (2020) characterise adversarial models to motivate their designs but include no risk assessment.

Article 21(1) of the NIS 2 Directive requires member states to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage risks to the security of the network and information systems used for their operations or services (Directive 2022/2555, Art. 21(1)). The reviewed literature provides limited support for deriving forensic readiness requirements from such measures.

5.4.2 Operational Continuity and Preparedness

Five studies address continuity directly, eight indirectly, and two not at all.

The studies that do address it formulate continuity in terms of patient care, not business operation. Yaqub et al. (2026) make it a named readiness objective: acquisition must minimise disruption and avoid impacting patient care, with persistent writes bounded to the minimum required for staging. Cusack and Kyaw (2012) achieve the same property architecturally: the forensic element is independent and self-resourcing and can function without visibility, so that the cost to the clinical service is minimal.

Grispos et al. (2017) go further and model the conflict directly. In the event of an incident, medical requirements may demand that a component continue delivering its medical functionality, and this may conflict with the preservation and collection of evidential data. Their framework therefore requires stakeholders to identify the medical requirements first and then perform a trade-off analysis against forensic requirements. This is the only included study that treats the conflict between continued clinical function and evidence collection as a design decision requiring analysis rather than as a problem to be assumed away.

Mpungu et al. (2024) address continuity as infrastructure availability, specifying replication across nodes in a decentralised storage platform to support business continuity in the event of security incidents. Gombar et al. (2026) build their model on resilience work emphasising adaptive system recovery and operational continuity.

Article 21(2)(c) of the NIS 2 Directive includes business continuity, such as backup management and disaster recovery, and crisis management among the minimum cybersecurity risk-management measures (Directive 2022/2555, Art. 21(2)(c)). Two included studies provide no continuity evidence at all.

5.4.3 Incident Response and Recovery

Six studies address incident response directly, while nine support post-incident investigation without specifying response or recovery procedures. Among the direct treatments, Mpungu et al. (2024) specify tiered incident response team classes, with escalation determined by severity, and alerting from both the security information and event management system and the behavioural analytics layer. Kyaw et al. (2019, 2020) specify automated active response through OSSEC scripts triggered by security alerts, alongside intrusion detection. Grispos et al. (2017) require specification of the circumstances under which escalation to a full formal investigation should be launched, supported by an incident response taxonomy grading severity and impact. Bankole et al. (2022) require an incident escalation policy and specification of how intrusion detection triggers should function and respond.

Gombar et al. (2026) treat recovery differently from every other included study. Their concept of adaptive recovery treats recovery not as a terminal step but as a feedback loop: recovery is evidence-informed and

feeds back into detection thresholds, response prioritisation and resilience planning, so that forensic learning from one incident improves the response to the next.

The nine indirect treatments share a pattern: the approach supports investigation after an incident but specifies no detection, containment or recovery action. This is a consistent property of the reviewed literature rather than an oversight in particular studies.

5.5 Healthcare-Specific and General Forensic Readiness Compared

The search string combined forensic readiness terminology with healthcare terminology, so the fifteen included studies represent the intersection of two literatures. Chapter 2 presented the broader general forensic readiness literature. Comparing the two shows which general approaches are taken up in healthcare contexts and which are not.

Foundational work carries into healthcare; several later organisational frameworks do not. Rowlingson's (2004) ten-step process is adopted directly by Grispos et al. (2017), whose framework activities are drawn from it, and adapted by Gombar et al. (2026) into survey indicators. ISO/IEC 27043 structures Mpungu et al. (2024) and informs Kyaw et al. (2019). By contrast, several organisational frameworks presented in the general literature—Reddy and Venter (2013), Elyas et al. (2015), Englbrecht et al. (2020), and Adel (2022)—are cited by none of the healthcare-specific included studies. Only Adel et al. (2024), itself an organisational framework, builds on that strand.

The two literatures have different strengths. The general approaches presented in Chapter 2 are stronger on governance: Reddy and Venter (2013) store the organisational hierarchy with responsibilities for all staff, Englbrecht et al. (2020) stage responsibility allocation across maturity levels, and Koen and Venter (2024) encode approver authority in machine-enforced policy. The healthcare-specific studies are stronger in the technical properties of evidence in constrained environments: volatile memory acquisition from devices that cannot be interrupted, edge capture where devices cannot retain logs, and attribution across heterogeneous medical device protocols.

A plausible explanation is the nature of the constraint each strand addresses. The general organisational frameworks answer the question of how an organisation should be arranged to be forensically ready. The healthcare studies answer the question of how evidence can be obtained at all from devices that restrict logging, execution and investigator access to preserve certification posture (Yaqub et al., 2026), or that exhibit limited memory, proprietary firmware and intermittent connectivity (Al-Balasmeh, 2026). Where the technical problem is unsolved, the organisational problem is not yet the binding constraint.

This has a consequence visible in the results. Four included studies provide no governance evidence at all, and three of those four are designed for hospital environments. Within the reviewed studies, the healthcare-specific literature shows a strong technical focus and less coverage of the organisational layer developed in the general literature.

5.6 Synthesis

The complete evidence is given in Appendix B, the cross-study evidence matrix is provided in Appendix C, and the distribution of codes is summarised in Table 8.

Table 8
Distribution of evidence by requirement and dimension

Dimension	Requirement	Direct	Indirect	Not evidenced	% Direct
Accountability	A1 Logging and monitoring	14	0	1	93%
Compliance	C3 Evidence preservation and data minimisation	13	2	0	87%
Accountability	A3 Traceability and identification	11	4	0	73%
Compliance	C2 Interoperability and technical standards	8	7	0	53%
Compliance	C1 Data protection and privacy	7	8	0	47%
Accountability	A2 Responsibility and governance	7	4	4	47%
Cyber resilience	CR3 Incident response and recovery	6	9	0	40%
Cyber resilience	CR1 Risk management	5	8	2	33%
Cyber resilience	CR2 Operational continuity and preparedness	5	8	2	33%
	Compliance total	28	17	0	62.2%
	Accountability total	32	8	5	71.1%
	Cyber resilience total	16	25	4	35.6%
	All requirements	76	50	9	56.3%

5.6.1 Recurring Patterns Across the Included Studies

Two capabilities are near-universal. Logging and monitoring is directly evidenced by fourteen of fifteen studies, and evidence preservation by thirteen. These constitute the settled core of what the healthcare forensic readiness literature offers. The mechanisms recur across environments as different as an ultrasound device, a hospital wireless network and a fog-enabled cloud, suggesting that the literature has converged on recurring mechanisms for capturing and protecting evidence, even though deployment-specific difficulties remain.

The ordering of support contrasts with the healthcare priorities identified in this study. Accountability is best supported at 71.1% direct, compliance next at 62.2%, and cyber resilience weakest at 35.6%. In a clinical setting, the availability of systems is connected to patient safety (Kruse et al., 2017), and the capacity to continue delivering care during and after an incident is a precondition for the other requirements rather than one among them. The reviewed literature is strongest in the evidential capabilities that support investigation after the fact and weakest in the resilience capabilities that determine whether care continues while an incident unfolds.

Risk assessment is treated as work completed elsewhere. In ten of fifteen studies, risk appears as motivation for the approach rather than as a component from which readiness requirements are derived. This follows the scoping decision Rowlingson (2004) made at the origin of the field, where a risk assessment is assumed to have been performed and appropriate defensive measures are assumed to be in place. The assumption has propagated: the reviewed literature largely inherits it rather than examining it.

5.6.2 Differences in Emphasis Between Approaches

Two types of approach emerge, with contrasting blind spots. Component-level technical designs—Cusack and Kyaw (2012), Kyaw et al. (2019, 2020), Mishra and Bagade (2022), Al-Balasmeh (2026), and Janjua et al. (2020) specify in detail what a system captures, how integrity is assured, and how evidence is

stored, but four of them specify no responsible party. Organisation-oriented approaches, such as Adel et al. (2024) and Bankole et al. (2022), specify roles, policies and separation of duties, but Adel et al. (2024) specify no logging mechanism at all. Neither type is complete on its own.

Data protection divides by what is protected, not by environment. Seven studies protect the data subject through encryption applied to health data, anonymisation, privacy-enhancing technologies or architectural decisions about what enters permanent storage. Eight protect the network on which patient data travels or detect modification of the record. Both are security measures; only the first addresses the patient as a data subject rather than merely protecting the surrounding infrastructure.

Continuity carries two distinct meanings. Three studies formulate it as continuity of clinical function: acquisition must not impact patient care, or the forensic element must operate independently of the clinical service. Two formulate it as availability of infrastructure through replication or resilience mechanisms. These are not degrees of the same property, and a healthcare organisation would need to distinguish them.

5.6.3 Complementary Capabilities

The included studies are complementary in a way that is visible when they are read together rather than separately.

Adel et al. (2024) define eight investigative positions with individual obligations, but the framework specifies no mechanism generating the evidence those positions would examine. Kyaw et al. (2020) aggregate logs from eight components in a hospital wireless network, including application-layer activity within the electronic medical record, and do not allocate responsibility to a defined role. Read together, they specify a workable capability; read separately, each has a gap the other fills.

The same complementarity appears across dimensions. Grispos et al. (2017) require a trade-off analysis between medical and forensic requirements but specify no acquisition mechanism. Yaqub et al. (2026) specify a volatile-first acquisition workflow that bounds its own footprint but do not address who authorises its use beyond stating that the framework assumes authorisation and governance. Al-Balasmeh (2026) resolves the tension between blockchain immutability and patient privacy by keeping raw artefacts off-chain, a decision that none of the other blockchain-based studies makes.

Four studies span both the technical and organisational dimensions: Grispos et al. (2017), Mpungu et al. (2024), Gombar et al. (2026) and Mekala et al. (2025). These are also among the studies with the highest counts of direct evidence, and three of the four address healthcare or a healthcare-relevant environment directly.

5.6.4 Healthcare-Specific Characteristics

Four properties appear in the healthcare-specific studies and in none of the others.

Patient safety as the continuity constraint. Yaqub et al. (2026), Grispos et al. (2017) and Cusack and Kyaw (2012) define continuity in terms of clinical function rather than service availability or financial loss. Mishra and Bagade (2022) identify the stakes concretely: pausing or adjusting drug administration in an insulin pump application can jeopardise patient safety, and adverse events in pacemakers may result in cardiac failure.

Authorised access as the dominant threat. Chernyshev et al. (2019) focus on privilege abuse because internal actors account for most healthcare breach incidents. Mpungu et al. (2024) demonstrate attribution of a clinician's actions. Zehra et al. (2024) demonstrate impersonation of a registered doctor experimentally.

Regulatory and device constraints on collection. Yaqub et al. (2026) observe that regulated medical devices restrict logging, execution and investigator access to preserve certification posture, so that the systems most in need of forensic visibility are least able to provide it. Al-Balasmeh (2026) identifies that medical IoT devices exhibit limited memory, proprietary firmware and intermittent connectivity, invalidating the assumptions of centralised retention that conventional forensics makes.

Physiological data as a forensic ambiguity. Mishra and Bagade (2022) note that a change in a patient's physiological readings may be an attack or a genuine clinical change, and that distinguishing between them is a forensic problem. This arises only in medical systems, and no other included study addresses it.

5.6.5 Overall Findings

Taken collectively, the included studies establish the following.

Requirements the literature supports. Logging and monitoring is supported by fourteen of fifteen studies, with mechanisms specified for environments ranging from electronic medical records to resource-constrained medical IoT devices. Evidence preservation is supported by thirteen studies, with converging mechanisms that transfer across environments. The traceability and identification requirement is supported by eleven studies, three of which demonstrate attribution of an authorised user's actions in a healthcare context.

Requirements the literature supports unevenly. Data protection is directly supported by seven studies, but the eight indirect treatments protect the infrastructure rather than the data subject. The interoperability and standards requirement is directly supported by eight studies anchored on ISO/IEC 27043, but no study engages with a healthcare-sector interoperability standard. The responsibility and governance requirement is directly supported by seven studies and entirely absent from four, all of which are component-level technical designs and three of which are designs for hospital environments.

Requirements the literature supports weakly. Risk management is directly supported by five studies; in the remaining ten, it appears as motivating context rather than as a component. Operational continuity is directly supported by five studies and absent from two. Incident response is directly supported by six studies, while nine support investigation after an incident without specifying detection, containment or recovery action.

5.6.6 Remaining Gaps

Seven gaps emerge from the evidence. These describe limitations in what the reviewed literature currently supports, rather than what the approaches could potentially be extended to support. The gaps are labelled using the abbreviation G.

G1. Data minimisation is largely unaddressed. Only four of the fifteen studies engage with data minimisation, and none frames the amount of personal data processed in the terms required by Article 5(1)(c) of the GDPR. Two studies even take positions that work against this requirement. This reflects a basic tension between forensic readiness and data protection: readiness favours retaining data because its evidential value may not be known in advance, while data protection requires personal data to be limited to what is necessary for the purpose.

G2. Logging focuses on modifications rather than access. Chernyshev et al. (2019) report that most electronic medical record systems do not log viewing activity. The only included study that reaches the clinical application layer captures logins and setting changes rather than access to individual records. This is significant in the Swedish context because the Swedish Patient Data Act requires automated access to patient data to be documented and checkable (SFS 2008:355, 4 kap. 3 §), while HSLF-FS 2016:40 requires systematic and recurring sample-based review of access logs (HSLF-FS 2016:40, 4 kap. 9 b §).

G3. Data protection often focuses on the network rather than the data subject. Eight of the fifteen studies secure the infrastructure carrying patient data or detect changes to the record, but do not address how patient data is protected from unauthorised viewing. This leaves an important distinction between protecting the system and protecting the person whose data the system contains. Data concerning health are also classified as a special category of personal data under Article 9(1) of the GDPR (Regulation 2016/679, Art. 9(1)).

G4. Governance is missing from the technical designs. Four studies provide no evidence of responsibility or governance, three of which are designed for hospital environments. This is difficult to reconcile with the governance requirements of the NIS 2 Directive, under which Article 20(1) assigns approval and oversight responsibilities to management bodies. The technical designs specify what should happen, but they do not specify who is responsible for implementation.

G5. Risk management rarely forms the basis for forensic readiness requirements. Only five of the fifteen studies derive readiness from an assessed risk. In the remaining studies, risk is generally used to motivate the approach rather than to determine what the approach should provide. This contrasts with Article 21(1) of the NIS 2 Directive, which requires risk-management measures.

G6. Continuity is rarely considered together with evidence collection. Only one included study treats the conflict between maintaining medical functionality and acquiring forensic evidence as a problem that requires an explicit trade-off analysis. The other approaches generally address continuity either by limiting the impact of evidence collection or by maintaining infrastructure availability, without examining the two requirements together.

G7. Healthcare requirements are not used to derive the models. None of the included studies derives its requirements from healthcare-sector legislation, and none reports implementation in an operational healthcare setting. No included study cites Patientdatalag, the EHDS Regulation or the NIS 2 Directive as a basis for its design. Instead, the direction of development generally runs from general forensic principles towards application in healthcare. The literature shows how existing forensic readiness ideas can be used in healthcare, but not how healthcare's legal and practical needs should guide their development from the beginning.

6 Discussion

This chapter interprets the results reported in Chapter 5 in relation to the study's aim and research question: "Which requirements related to compliance, accountability and cyber resilience within the Swedish healthcare sector are supported by existing Digital Forensic Readiness (DFR) models and frameworks, and which gaps remain?" Section 6.1 relates the findings to the conceptual framework and to previous research, while Section 6.2 discusses their ethical and societal implications. The interpretation of these findings should be considered together with the validity and reliability measures described in Section 4.3, particularly the defined search scope and the consistent coding framework applied across the included studies.

6.1 In relation to previous research

This subsection relates the findings to the conceptual framework, previous digital forensic readiness research and healthcare cybersecurity research.

6.1.1 Relation to the Conceptual Framework

The analysis used three dimensions, compliance, accountability and cyber resilience, derived from the legal instruments governing Swedish healthcare and operationalised into nine requirements. Following Jabareen (2009), these function as a conceptual framework: a set of interlinked concepts providing an interpretation of a phenomenon rather than a causal explanation. They were applied deductively, in the sense described by Braun and Clarke (2006), with the themes fixed before the studies were read and sub-coding used to permit the more detailed interpretation described by Saldaña (2013).

The results bear on the framework in two ways that were not anticipated when the dimensions were defined.

The three dimensions were not equally tractable. Compliance and accountability decomposed into requirements that could be recognised consistently in the reviewed texts: a study either names a logging component or it does not. Cyber resilience decomposed less cleanly. Continuity in particular carried two distinct meanings across the included studies: continuity of clinical function and availability of infrastructure, which are not degrees of the same property. Linkov and Kott (2018) define resilience as the capacity to maintain essential functions under disruption, but the studies disagree about which function is essential.

The compliance dimension contained an internal tension. Evidence preservation and data minimisation were grouped under one requirement because both derive from obligations governing evidence handling. The results showed an almost inverse distribution: thirteen studies address preservation, while four address minimisation. This is consistent with the derivation, since Article 5(1)(c) of the GDPR and the evidential provisions of Patientdatalag do impose both, but it indicates that the requirement grouped two obligations that pull against each other. Separating them, as the coding rules required, is what made the finding visible.

Neither observation invalidates the framework. Both suggest that a conceptual framework derived from legal obligations will not necessarily align with how a technical literature organises itself, and the misalignment is itself informative.

6.1.2 Relation to Previous Digital Forensic Readiness Research

Several included studies report a shortfall in the environment they address. Chernyshev et al. (2019) state that digital investigations of incidents involving health information are often constrained by a lack of forensic readiness infrastructure. Yaqub et al. (2026) describe a recurring forensic blind spot in clinical incident response. Grispos et al. (2017) note the limited research addressing comprehensive design considerations for medical cyber-physical systems. Al-Balasmeh (2026) observes that conventional forensic methodologies assume centralised retention and comprehensive logging, assumptions that do not hold in medical IoT environments.

Each observation is made from within a single environment. The contribution of this study is comparative: applying one coding framework across fifteen studies establishes that certain shortfalls are not local to the environment in which they were noticed. Risk management is weakly supported across the whole included set, not only in medical devices. Data minimisation is weakly supported across the whole set, not only in electronic medical records.

The results also explain a pattern the literature has noted without measuring. Elyas et al. (2015) note the lack of guides and standards for forensic readiness; Adel (2022) reports the view that privacy standards for forensic infrastructure remain to be developed. The coded results quantify this pattern: eight of fifteen studies name a standard, ISO/IEC 27043 is the only one appearing more than twice, and none is healthcare-sector specific.

One result stands in tension with the foundational literature rather than conforming to it. Rowlingson (2004), whose ten-step process most subsequent work builds upon, excludes preventive and recovery measures from the definition of forensic readiness and assumes a prior risk assessment. The results show this assumption propagating: ten of fifteen included studies treat risk as work completed elsewhere. A scoping decision made at the origin of the field continues to shape what it addresses two decades later.

6.1.3 Relation to Healthcare Cybersecurity Research

The results are consistent with what the wider healthcare cybersecurity literature reports about the sector's exposure. Kruse et al. (2017) document the connection between the availability of clinical systems and patient safety; ENISA (2023) reports ransomware as the dominant incident type in the European healthcare sector; Moore et al. (2023) describe the operational consequences of the attack on Ireland's Health Service Executive, where the loss of ICT systems forced staff onto paper-based workarounds.

What the results add is a specific point of contact between that literature and the forensic readiness literature. The healthcare cybersecurity literature establishes that availability is a safety property in this sector. The results establish that continuity is among the weakest-supported requirements in the forensic readiness literature, and that only three included studies formulate it in patient-safety terms. The healthcare cybersecurity literature identifies the property as critical, while the forensic readiness literature leaves it under-addressed.

A second point of contact concerns the threat model. Chernyshev et al. (2019) report that internal actors account for most healthcare breach incidents. Most technical approaches assume an external adversary who must first gain access. Zehra et al. (2024) demonstrate the healthcare version experimentally: an attacker exploiting a missing access check impersonates a registered doctor, deletes records added by a verified doctor, and adds falsified reports that the patient subsequently sees. Where the healthcare literature identifies the insider as the dominant threat, the forensic readiness literature has largely not been designed around it.

The corpus contains three structurally different responses to the problem of the privileged insider, and no included study compares them. Janjua et al. (2020) make multi-stakeholder collusion technically infeasible through ownership non-repudiation and homomorphic encryption. Al-Balasmeh (2026) anchors custody events on a permissioned ledger so that handling cannot be retrospectively altered. Bankole et al. (2022) separate the approval of an investigation from its execution. For a Swedish care provider, where the person to be held accountable may also administer the systems producing the evidence, these represent materially different levels of assurance, and the literature offers all three while comparing none.

6.2 Ethical and societal aspects

The results describe capabilities that, if implemented, could monitor the activities of clinical staff and collect data concerning patients. This section discusses the ethical and societal implications of these capabilities.

6.2.1 Forensic Readiness in Healthcare Is a Form of Workplace Monitoring

The best-supported capability in this review is logging and monitoring. In a healthcare setting, what is logged is the activity of nurses, physicians, administrators and technicians, and what is monitored is their access to patient records. Chernyshev et al. (2019) make this explicit: the architecture they propose captures the artefacts needed to investigate privilege abuse, and the use cases include detecting access to the records of colleagues, neighbours, family members and high-profile individuals.

Rowlingson (2004) recognised the issue at the origin of the field, citing the position that monitoring should be targeted at specific problems, that data should be gathered for defined purposes and nothing more, and that staff should be told what monitoring is taking place except in exceptional circumstances. This remains the only treatment in the reviewed literature that addresses the monitored person rather than the monitoring organisation.

The societal implication is that a capability justified as protecting patients also expands an employer's visibility over its workforce. In a sector where clinical staff already work under a significant documentation burden, comprehensive access logging is not ethically neutral. Two mitigations appear in the results. Rowlingson's transparency principle is procedural. Al-Balasmeh (2026) offers a technical one, keeping raw artefacts off the immutable ledger so that what is permanently recorded is limited to integrity anchors and custody metadata. The latter more directly limits exposure because it restricts what is retained rather than only disclosing that retention occurs.

6.2.2 The Minimisation Gap Has Consequences for Patients

The results showed that four of fifteen studies address data minimisation. This was reported in Chapter 5 as a compliance gap. It is also an ethical one.

A forensic readiness capability that captures broadly and retains indefinitely increases the volume of sensitive data held about patients and the number of people with access to it. Grispos et al. (2017) identify the resulting exposure directly, noting that private patient information generated through ordinary use of a medical cyber-physical system could be exposed to forensic investigators examining a security incident, and that privacy requirements may therefore conflict with forensic strategies.

Yaqub et al. (2026) demonstrate the concrete form this takes: their memory analysis recovered structured patient logs and renderable diagnostic images from device memory. Evidence collected to investigate a security incident contained clinical material about identifiable patients who had no involvement in that incident.

The ethical question is therefore not whether forensic readiness is compatible with data protection in principle, but who bears the cost of the tension. The organisation gains investigative capability; the patient bears the increased exposure. Adel et al. (2024) address that trade-off explicitly by requiring the exclusion of irrelevant data from reports. Most included studies do not raise the question.

6.2.3 Designing Around the Insider Affects Trust

Authorised-user misuse is a prominent threat in the healthcare literature considered in this review, and several of the approaches most relevant to that threat are designed on the assumption that an authorised user may be untrustworthy.

These designs respond directly to the threat model, but they also encode an institutional stance towards staff. A system that treats clinicians as potential subjects of investigation, and administrators as parties who might tamper with the record, changes the relationship between an organisation and the people delivering care within it.

Healthcare depends on professional trust in ways that differ from many other sectors. Adel et al. (2024) discuss bias and objectivity as ethical issues in forensic investigation, noting that findings must rest solely on evidence and that bias can lead to wrongful accusations and undermine the credibility of the investigation. If such a system is deployed in an environment of low trust, or where its outputs are used for performance management rather than incident investigation, the same evidence that protects patients could be used in ways staff did not anticipate when it was collected. No included study addresses the governance of secondary use of forensic evidence.

6.2.4 Capability Is Not Distributed Equally

Chernyshev et al. (2019) observe that a large proportion of smaller healthcare providers do not have an established information security capability and lack the incentive to find initiatives addressing auditable activity trails. Adel et al. (2024) note that forensic investigation is resource-intensive, requiring specialised hardware, software and skilled personnel, and that smaller organisations may lack the resources to conduct thorough investigations.

Taken together, these observations suggest that the capabilities identified in this review may be easier for well-resourced providers to implement than for smaller primary care practices, private providers or municipal care services. This is an inference from the resource constraints reported in the reviewed literature, not a direct comparison of Swedish healthcare providers. The access-verification duty in the Patient Data Act is framed as a duty on healthcare providers and does not distinguish that duty by provider size (SFS 2008:355, 4 kap. 3 §). Unequal organisational resources may therefore contribute to differences in practical capacity to meet the same obligation.

6.2.5 Relation to the Sustainable Development Goals

The results connect to three of the United Nations Sustainable Development Goals, in each case indirectly and through healthcare delivery rather than through forensic readiness as such.

Goal 3, Good Health and Well-being. The connection runs through availability. Where cyberattacks disrupt clinical systems, care delivery is impaired (Moore et al., 2023; ENISA, 2023). The results bear on this in a qualified way: continuity, the capability most directly connected to sustained care delivery, is among the weakest-supported in the review.

Goal 16, Peace, Justice and Strong Institutions, and specifically target 16.6 concerning effective, accountable and transparent institutions. This is the closest connection. Accountability was the best-supported dimension, and the capacity to establish who accessed patient data, when, and under what authority constitutes an institutional accountability mechanism. The Swedish Patient Data Act expresses the same principle in national law.

Goal 9, Industry, Innovation and Infrastructure, in relation to resilient infrastructure. NIS 2 lists health as a sector of high criticality in Annex I, point 5, including healthcare providers; whether an organisation is within scope and classified as essential or important is determined under Articles 2 and 3 (Directive 2022/2555, Arts. 2–3, Annex I, point 5). Sweden is also implementing a national digital infrastructure in preparation for mandatory exchange of certain health data categories from March 2029 (E-hälsomyndigheten, 2025; Regulation 2025/327, Art. 105). The results indicate limited support here: no included study engages with healthcare-sector interoperability standards.

7 Conclusion

The aim of this study is to answer the research question "Which requirements related to compliance, accountability and cyber resilience within the Swedish healthcare sector are supported by existing Digital Forensic Readiness (DFR) models and frameworks, and which gaps remain?"

Nine requirements were derived from the General Data Protection Regulation, the Network and Information Security 2 Directive, the Cyber Resilience Act, the European Health Data Space Regulation, the Swedish Patient Data Act and its supporting regulations. A structured literature review across seven databases identified fifteen studies meeting the inclusion criteria, which were analysed against the nine requirements using a coding framework defined before the analysis began.

The requirements are supported unevenly, and the pattern of support contrasts with the healthcare priorities identified in this study. Accountability is the best-supported dimension, at 71.1% direct evidence: logging and monitoring is addressed directly by fourteen of fifteen studies, and traceability by eleven. Across all requirements, evidence preservation is also strongly supported, with direct evidence in thirteen studies. Compliance is supported at 62.2%. Cyber resilience is the weakest, at 35.6%; risk management and operational continuity are each addressed directly by five studies. In a clinical setting, where the availability of systems is connected to patient safety, the capacity to continue delivering care during an incident is a precondition for the other requirements rather than one among them. The literature is strongest in the capabilities that support investigation after the fact and weakest in those that determine whether care continues while an incident unfolds.

Three findings are specific to the Swedish healthcare context. First, the reviewed approaches log the creation and modification of records more reliably than access to them, while the Swedish Patient Data Act requires automated access to patient data to be documented and checkable (SFS 2008:355, 4 kap. 3 §), and HSLF-FS 2016:40 requires systematic and recurring sample-based review of access logs (HSLF-FS 2016:40, 4 kap. 9 b §). Second, data protection in these approaches generally secures the network carrying patient data rather than the patient as a data subject, which is a material distinction for special-category data under Article 9 of the GDPR. Third, four included studies specify no responsible party for the readiness capability at all, three of them being designs for hospital environments, while Article 20(1) of the NIS 2 Directive requires management bodies to approve and oversee cybersecurity risk-management measures.

Comparing the healthcare-specific literature with the general forensic readiness literature shows a divided uptake. Foundational work carries into healthcare: Rowlingson's ten-step process and ISO/IEC 27043 are adopted by several healthcare studies. The later organisational frameworks that are prominent in the general literature presented in Chapter 2 are cited by none of the healthcare-specific studies. The healthcare-specific studies focus strongly on technical constraints, such as evidence acquisition from devices that restrict logging and cannot be interrupted, while providing less coverage of the organisational layer developed in the general literature.

No included study derives its requirements from healthcare-sector legal obligations, and none has been implemented in an operational healthcare setting. The direction of derivation throughout the reviewed literature runs from general forensic principles towards application in a healthcare environment, not from healthcare obligations towards design.

The study answers the research question by establishing what the reviewed literature specifies, not what it achieves in practice. A Swedish care provider consulting this literature would find comparatively strong guidance on evidence preservation, logging and attribution. Such a provider would still need to supply the risk-management derivation, sectoral legal mapping and clinical continuity analysis itself.

7.1 Contribution

The study makes three contributions.

First, it provides a structured mapping between healthcare-sector legal requirements and forensic readiness capability. Nine requirements derived from six legal instruments were operationalised into a coding framework and applied to fifteen studies, producing a traceable account of which requirements the literature supports and where it does not.

Second, it provides an auditable coding procedure for comparing forensic readiness approaches. Every coding decision is supported by evidence from the reviewed article and its assigned code is reported in Appendix B, so that the analysis can be examined against the evidence rather than accepted on assertion.

Third, it provides a comparison between healthcare-specific and general forensic readiness literature. The study shows which general approaches are taken up in healthcare contexts and which are not, and offers an explanation grounded in the constraints each strand addresses.

7.2 Future work

Empirical implementation. The most significant gap in the reviewed literature is that no approach has been deployed in an operational healthcare setting. Research implementing one of the identified approaches in a Swedish care provider, and measuring both the capability obtained and the operational impact on clinical work, would establish what this review cannot.

A forensic readiness approach derived from healthcare obligations. No reviewed approach begins from healthcare-sector legal requirements. Design-oriented research developing an approach from Patientdatalag, the EHDS Regulation and the NIS 2 Directive outward, rather than adapting a general model to healthcare afterwards, would address the derivation gap identified here. The results of this study provide the requirements such work would need.

Logging of access rather than modification. The finding that electronic medical record systems commonly log modification but not viewing, combined with the access-verification obligation in the Patient Data Act and the log-checking requirements in HSLF-FS 2016:40, identifies a specific and addressable technical gap. Research establishing what access logging in clinical systems would need to capture, and at what operational cost, would be directly applicable.

Reconciling continuity with evidence collection. Only one included study models the conflict between continued clinical function and forensic acquisition as a design decision requiring analysis. Research developing that trade-off analysis into a usable method would address a requirement that healthcare cannot avoid.

Empirical study of Swedish practice. This study analysed published models rather than practice. What Swedish care providers currently do, what forensic readiness capabilities they possess, and how they satisfy the access-verification obligation remain unknown from this evidence and could be established through interviews or survey research.

References

Adel, A. (2022). A conceptual framework to improve cyber forensic administration in Industry 5.0: Qualitative study approach. *Forensic Sciences, 2*(1), 111–129. https://doi.org/10.3390/forensicsci2010009

Adel, A., Ahsan, A., & Davison, C. (2024). ETHICore: Ethical compliance and oversight framework for digital forensic readiness. *Information, 15*(6), 363. https://doi.org/10.3390/info15060363

Adler-Milstein, J., Holmgren, A. J., Kralovec, P., & Worzala, C. (2017). Electronic health record adoption in US hospitals: The emergence of a digital "advanced use" divide. *Journal of the American Medical Informatics Association, 24*(6), 1142–1148. https://doi.org/10.1093/jamia/ocx080

Al-Balasmeh, H. (2026). Edge-based digital forensics for medical IoT with permissioned blockchain verification. In *Proceedings of the 39th Conference of the Open Innovations Association FRUCT* (pp. 18–27). FRUCT Oy. https://doi.org/10.23919/FRUCT70069.2026.11506557

Albugmi, A. (2024). Digital forensics readiness framework (DFRF) to secure database systems. *Engineering, Technology & Applied Science Research, 14*(2), 13732–13740. https://doi.org/10.48084/etasr.7116

Alnajjar, I. A., Salameh, A. A., Almazaydeh, L., & Al Tawil, A. (2026). Two-tier forensic readiness architecture for Zero Trust-enabled Industry 4.0 applications. *Information Security Journal: A Global Perspective, 35*(3), 363–380. https://doi.org/10.1080/19393555.2025.2528065

Baiquni, I. Z., & Amiruddin, A. (2022). A case study of digital forensic readiness level measurement using DiFRI model. In *2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* (pp. 184–189). IEEE. https://doi.org/10.1109/ICIMCIS56303.2022.10017686

Bankole, F. O., Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation, 40*, 301348. https://doi.org/10.1016/j.fsidi.2022.301348

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis projects: A guide for students in computer science and information systems* (2nd ed.). Springer. https://doi.org/10.1007/978-1-84800-009-4

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems, 43*(1), 7. https://doi.org/10.1007/s10916-018-1123-2

Cusack, B., & Kyaw, A. K. (2012). Forensic readiness for wireless medical systems. In *Proceedings of the 10th Australian Digital Forensics Conference* (pp. 25–28). Edith Cowan University. https://doi.org/10.4225/75/57b3af0efb860

Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023a). Addressing insider attacks via forensic-ready risk management. *Journal of Information Security and Applications, 73*, 103433. https://doi.org/10.1016/j.jisa.2023.103433

Daubner, L., Matulevičius, R., & Buhnova, B. (2023b). A model of qualitative factors in forensic-ready software systems. In J. Araújo, J. L. de la Vara, M. Y. Santos, & S. Assar (Eds.), *Research challenges in information science: Information science and the connected world* (Lecture Notes in Business Information Processing, Vol. 476, pp. 308–324). Springer. https://doi.org/10.1007/978-3-031-33080-3_19

Directive 2022/2555. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). http://data.europa.eu/eli/dir/2022/2555/oj

E-hälsomyndigheten. (2025). *E-hälsomyndigheten föreslår en nationell digital infrastruktur för delning av hälsodata* https://www.ehalsomyndigheten.se/om-ehalsomyndigheten/aktuellt/nyheter/2025/e-halsomyndigheten-foreslar-en-nationell-digital-infrastruktur-for-delning-av-halsodata/

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a

theoretical framework. *Computers & Security, 52*, 70–89. https://doi.org/10.1016/j.cose.2015.04.003

Englbrecht, L., Meier, S., & Pernul, G. (2020). Towards a capability maturity model for digital forensic readiness. *Wireless Networks, 26*(7), 4895–4907. https://doi.org/10.1007/s11276-018-01920-5

European Union Agency for Cybersecurity. (2023). *Checking up on health: Ransomware accounts for 54% of cybersecurity threats* https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats

Fagbola, F. I., & Venter, H. S. (2022). Smart digital forensic readiness model for shadow IoT devices. *Applied Sciences, 12*(2), 730. https://doi.org/10.3390/app12020730

Gombar, M., Možnik, D., & Pejić Bach, M. (2026). Anomaly detection as a key driver of digital forensic resilience: Empirical evidence from critical infrastructure experts. *Systems, 14*(2), 213. https://doi.org/10.3390/systems14020213

Grispos, G., Glisson, W. B., & Choo, K.-K. R. (2017). Medical cyber-physical systems development: A forensics-driven approach. In *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)* (pp. 108–113). IEEE. https://doi.org/10.1109/CHASE.2017.68

Health Service Executive. (2021). *Conti cyber attack on the HSE: Independent post incident review* https://about.hse.ie/publications/conti-cyber-attack-on-the-hse-independent-post-incident-review/

HSLF-FS 2016:40. Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården [The National Board of Health and Welfare's regulations and general advice on record-keeping and the processing of personal data in healthcare]. https://www.socialstyrelsen.se/kunskapsstod-och-regler/regler-och-riktlinjer/foreskrifter-och-allmanna-rad/konsoliderade-foreskrifter/201640-om-journalforing-och-behandling-av-personuppgifter-i-halso--och-sjukvarden/

International Organization for Standardization & International Electrotechnical Commission. (2015). *Information technology — Security techniques — Incident investigation principles and processes (ISO/IEC 27043:2015)* https://www.iso.org/standard/44407.html

Islam, S., Papastergiou, S., & Mouratidis, H. (2022). A dynamic cyber security situational awareness framework for healthcare ICT infrastructures. In *PCI '21: Proceedings of the 25th Pan-Hellenic Conference on Informatics* (pp. 334–339). ACM. https://doi.org/10.1145/3503823.3503885

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods, 8*(4), 49–62. https://doi.org/10.1177/160940690900800406

Janjua, K., Shah, M. A., Almogren, A., Khattak, H. A., Maple, C., & Din, I. U. (2020). Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-cloud using Holochain and containerization technologies. *Electronics, 9*(7), 1172. https://doi.org/10.3390/electronics9071172

Jiménez, M. B., Fernández, D., Rivadeneira, J. E., & Flores-Moyano, R. (2024). A filtering model for evidence gathering in an SDN-oriented digital forensic and incident response context. *IEEE Access, 12*, 75792–75808. https://doi.org/10.1109/ACCESS.2024.3405588

Kebande, V. R., & Venter, H. S. (2019). A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. *WIREs Forensic Science, 1*(6), e1350. https://doi.org/10.1002/wfs2.1350

Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K.-K. R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Science International: Reports, 2*, 100117. https://doi.org/10.1016/j.fsir.2020.100117

Koen, R., & Venter, H. (2024). A federated distributed digital forensic readiness model for the cloud. In *Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024)* (pp. 472–480). https://doi.org/10.34190/iccws.19.1.2175

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1–10. https://doi.org/10.3233/

THC-161263

Kyaw, A. K., Cusack, B., & Lutui, R. (2019). Digital forensic readiness in wireless medical systems. In *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ITNAC46935.2019.9078005

Kyaw, A. K., Tian, Z., & Cusack, B. (2020). Design and evaluation for digital forensic ready wireless medical systems. In G. Marques, A. Kumar Bhoi, & K. Hareesha (Eds.), *IoT technologies for HealthCare* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 314, pp. 118–141). Springer. https://doi.org/10.1007/978-3-030-42029-1_9

Linkov, I., & Kott, A. (2018). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer. https://doi.org/10.1007/978-3-319-77492-3_1

Mekala, S. H., Baig, Z., Anwar, A., Syed, N., & Zeadally, S. (2025). Securing the Industrial Internet of Things: A comprehensive digital forensic readiness framework and cybersecurity approach. *IT Professional, 27*(3), 29–37. https://doi.org/10.1109/MITP.2024.3498000

Mishra, A., & Bagade, P. (2022). Digital forensics for medical Internet of Things. In *2022 IEEE Globecom Workshops (GC Wkshps)* (pp. 1074–1079). IEEE. https://doi.org/10.1109/GCWkshps56602.2022.10008761

Moore, G., Khurshid, Z., McDonnell, T., Rogers, L., & Healy, O. (2023). A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. *BMC Health Services Research, 23*(1), 1112. https://doi.org/10.1186/s12913-023-10076-8

Mpungu, C., George, C. E., & Mapp, G. (2024). Enhancing digital forensics readiness in Big Data wireless medical networks: A secure decentralised framework. *International Journal of Network Security & Its Applications, 16*(4), 15–32. https://doi.org/10.5121/ijnsa.2024.16402

Office of the National Coordinator for Health Information Technology. (2025). *What are electronic health records (EHRs)? HealthIT.gov* https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-are-electronic-health-records-ehrs

Paré, G., & Kitsiou, S. (2017). Methods for literature reviews. In F. Lau & C. Kuziemsky (Eds.), *Handbook of eHealth evaluation: An evidence-based approach* (pp. 157–179). University of Victoria. https://www.ncbi.nlm.nih.gov/books/NBK481583/

Pisarenco, C., & Pisarenco, S. (2026). Forensic infrastructure for investigating medical crimes in the digital era. *Cadernos de Dereito Actual, 32*, 130–154. https://cadernosdedereitoactual.es/index.php/cadernos/article/view/1515

Rahman, A. F. A., Ahmad, R., & Ramli, S. N. (2014). Forensics readiness for wireless body area network (WBAN) system. In *16th International Conference on Advanced Communication Technology (ICACT)* (pp. 177–180). IEEE. https://doi.org/10.1109/ICACT.2014.6778944

Reddy, K., & Venter, H. S. (2013). The architecture of a digital forensic readiness management system. *Computers & Security, 32*, 73–89. https://doi.org/10.1016/j.cose.2012.09.008

Regulation 2016/679. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://data.europa.eu/eli/reg/2016/679/oj

Regulation 2024/2847. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). http://data.europa.eu/eli/reg/2024/2847/oj

Regulation 2025/327. 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. http://data.europa.eu/eli/reg/2025/327/oj

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence, 2*(3), 1–28. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

Saldaña, J. (2013). *The coding manual for qualitative researchers (2nd ed.)*. SAGE Publications.

SFS 2008:355. Patientdatalag [Patient Data Act]. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355/

Shahzadi, A., Ishaq, K., Dogar, A. B., Khan, J. A., Mylonas, A., Nawaz, N. A., Yasin, A., & Khan, F. A. (2025). Safeguarding the healthcare sector from ransomware attacks: Insights from a literature review. *PeerJ Computer Science, 11*, Article e3073. https://doi.org/10.7717/peerj-cs.3073

Sulaiman, R., Safanayasmin, K., Kesavan, R., & Pradeesh, S. (2026). Forensic readiness framework for evidence recovery in PaaS cloud databases. In *2026 6th International Conference on Intelligent Technologies (CONIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/CONIT69683.2026.11620751

Verizon. (2024). *2024 data breach investigations report* https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering*. Springer. https://doi.org/10.1007/978-3-642-29044-2

Yaqub, M. S., Jo, W., Nadeem, T., Topsakal, E., & Ahmed, I. (2026). Digital forensic readiness of regulated medical devices: An empirical study of the GE Venue ultrasound system. *Forensic Science International: Digital Investigation, 57*, 302121. https://doi.org/10.1016/j.fsidi.2026.302121

Zehra, F., Javed, M., Hyder, M. F., Darakhshan, & Tariq, S. M. A. (2024). Towards forensics investigation of blockchain-based healthcare applications. *IETE Journal of Research, 70*(5), 5053–5065. https://doi.org/10.1080/03772063.2023.2226106

A Retrieval of legal and regulatory instruments

Table A1
Legal and regulatory instruments used to derive the requirements

Instrument	Type	Jurisdiction	Source
Regulation 2016/679 (GDPR)	Regulation	European Union	EUR-Lex, consolidated text
Directive 2022/2555 (NIS 2)	Directive	European Union	EUR-Lex, consolidated text
Regulation 2024/2847 (Cyber Resilience Act)	Regulation	European Union	EUR-Lex, consolidated text
Regulation 2025/327 (EHDS)	Regulation	European Union	EUR-Lex, consolidated text
SFS 2008:355 (Patientdatalag)	Act	Sweden	Sveriges riksdag, consolidated text
HSLF-FS 2016:40	Regulation	Sweden	Socialstyrelsen

B Evidence extraction record

This appendix shows the evidence supporting every coding decision. Each entry gives the requirement, the evidence from the reviewed article and the assigned code. Quotations are verbatim; other entries are paraphrases of the reviewed article.

B.1 S1 – Chernyshev, Zeadally and Baig (2019)

Table B1
Evidence extraction for S1: Chernyshev, Zeadally and Baig (2019)

Req.	Evidence	Code
C1	"Availability of auditable action trails is crucial in safeguarding patient privacy and assisting with investigation of incidents involving privacy violations via means of privilege abuse. "	I
C2	"Subsequently, we leverage the established concept of forensic logging as a service (FaaS) to propose an audit logging architecture for EMR systems that is generic and EMR implementation-agnostic as shown in Fig. 4"	D
C3	"The FaaS component in the proposed architecture is based on the architectures described in [47, 48]. In particular, it de scribes a secure collection and preservation module, an examination and analysis module and a presentation module to support the remaining phases of the digital forensic process. In addition, the component features a provenance module which is responsible for guaranteeing the chain of custody and maintaining the record of artifact access and usage."	D
A1	"propose an audit logging architecture for EMR systems that is generic and EMR implementation-agnostic as shown in Fig. 4."	D
A2	" Therefore, sys tem architects must consider the concept of mandatory log events (MLEs) (forensics-enabling activities and actions) as part of the solution design and implementation"	I
A3	"Traces of actions performed by EMR users (or other connect ed services such as programmatic access clients) are expected to be captured in audit logs [41]"	D
CR1	"Table 5 Digital forensic readiness complexity levels for top healthcare threat types"	I
CR2	First, it does not require modification of the EMR system itself because it only requires the ability to inject payload analyzers across the various EMR system component communication channels which are often based on standard technological components	I
CR3	"The FaaS component in the proposed architecture is based on the architectures described in [47, 48]. In particular, it de scribes a secure collection and preservation module, an examination and analysis module and a presentation module to support the remaining phases of the digital forensic process."	I

B.2 S2 – Grispos, Glisson and Choo (2017)

Table B2
Evidence extraction for S2: Grispos, Glisson and Choo (2017)

Req.	Evidence	Code
C1	"privacy requirements may conflict with forensic strategies"	D
C2	"healthcare regulations and standards should also be considered"; "Furthermore, investigators tasked to investigate incidents in a MCPS must follow evidence handling procedures that adhere to digital forensics standards."	D
C3	"Establish a policy for secure storage and handling of potential evidence"Ensuring that potential evidence can be preserved and col lected both reliably and compliant with digital forensics standards."	D
A1	" Determine the evidence collection requirement." "As a result, cloudlets or gateway devices connected to the sensor need to collect and store event metadata in a database which can then examined, should the need arise."	D
A2	"Train staff in incident awareness, so that all those involved understand their role in the digital evidence process" "Furthermore, organizations need to define practices and policies that can be used"	D
A3	"Identify available sources and different types of potential evidence"	I
CR1	"identify potential incidents that can occur within a MCPS environment and then apply forensic readiness principles to these incidents"	D
CR2	"in the event of an incident or breach, medical requirements will likely demand that a component delivers its medical functionality. However, this could conflict with the preservation and collection of evidential data. Hence, stakeholders need to first identify the medical requirements for a MCPS and then perform a trade-off analysis between medical requirements with forensics-related requirements that support forensic readiness."	D
CR3	"Specify circumstances when escalation to a full formal investigation should be launched"	D

B.3 S3 – Yaqub, Jo, Nadeem, Topsakal and Ahmed (2026)

Table B3
Evidence extraction for S3: Yaqub, Jo, Nadeem, Topsakal and Ahmed (2026)

Req.	Evidence	Code
C1	"O5: Privacy-aware handling and reporting. Because volatile memory may contain PHI, readiness must include encryption, controlled access, retention limits, and reporting formats that separate privacy exposure assessment from security conclusions"	D
C2	"This work treats forensic readiness as an evidentiary problem rather than a compliance checklist."	I
C3	"O3: Integrity and provenance. Evidence must be verifiable through hashing, timestamp discipline, and detailed action logging that bounds the examiner footprint."	D
A1	"Provenance: action log, timestamps, cryptographic hashes; bound writes and footprint."	D
A2	"The framework assumes that evidence collection is conducted under authorization and governance, with explicit rules for PHI handling"	D
A3	"O6: Baseline-driven interpretation. Expected baselines for process lineage, loader chains, and core module sets reduce ambiguity and support deviation analysis when logging is sparse." chain	D
CR1	"We separate two capabilities that are often conflated in medical device security and forensic studies: an authorized examiner model and an adversary model."	I
CR2	"O4: Operational safety and minimal invasiveness. Acquisition must minimize disruption and avoid impacting patient care; persistent writes should be bounded to the minimum required for staging and should be documented."	D
CR3	"Overall, our results show that volatile acquisition is central to inci dent scoping "	I

B.4 S4 – Mpungu, George and Mapp (2024)

Table B4
Evidence extraction for S4: Mpungu, George and Mapp (2024)

Req.	Evidence	Code
C1	"Ensure compliance with data protection and privacy regulations. Assesses the impact of incidents on patient and employee data privacy during incidents."	D
C2	"The ISO/IEC's 27043:2015 incident investigation planning process guided the identification of requirements for the proposed framework	D
C3	"a write blocker (to ensure read-only access and preserve data integrity) is attached and the image is extracted using digital forensic software"	D
A1	"enables streamlined logging of evidential data within the BdDFR"	D
A2	"Table 2. Incident Response Team (IRT) "; Table 2 defines the incident response team	D
A3	". Authentication to the BdDFR is managed using IAM for internal users, and remote users are authenticated with an additional layer of blockchain-based authentication" "Concurrently, a UEBA (User and Entity Behaviour Analytics) system conducts a comprehensive analysis of all the data logs stored within the Hadoop cluster nodes. UEBA leverages advanced analytics and machine learning techniques to pinpoint deviations and patterns in behaviour, subsequently prioritizing alerts according to potential risk levels."	D
CR1	"Scenarios should be then defined based on the risk assessment analysis"	D
CR2	"provides fault tolerance by replicating data across multiple nodes … within a decentralised storage platform that supports business continuity (in case of security incidents)"	D
CR3	"guide security teams in responding to potential incidents promptly"	D

B.5 S5 – Mishra and Bagade (2022)

Table B5
Evidence extraction for S5: Mishra and Bagade (2022)

Req.	Evidence	Code
C1	" However, the medical devices are not equipped to use the latest technology due to low resources"	I
C2	"data collected from medical devices get transferred to the smartphone health app and then to the cloud over wireless channels using Wi-Fi, Bluetooth, Zigbee, etc"	I
C3	" Identification, preparation, isolation, preservation, processing of data, exam ination, verification, and reporting"	D
A1	"Forensic Readiness: The forensically-capable system should save logs for investigation and notify the user of the security breach."	D
A2	"Increased regulatory pressure needs to be applied to enterprises in the healthcare industry, requiring security incident capabilities"	NE
A3	"the acquired data contains information on the processes running in the system, their parent-child relationships, system logs, and event logs."	D
CR1	"Subsection III-A introduces the threat model for analyzing risks involved in the MIoT system", considering security and privacy needs, vulnerabilities, attack surfaces and countermeasures	D
CR2	" A patient's safety might get jeopardized by pausing and adjusting the drug administration in the smartphone app"	I
CR3	"organizations must identify these threats to implement proactive and reactive measures"	I

B.6 S6 – Al-Balasmeh (2026)

Table B6
Evidence extraction for S6: Al-Balasmeh (2026)

Req.	Evidence	Code
C1	"Raw artifacts remain securely stored off-chain to preserve privacy and scalability" "patient privacy protections under healthcare compliance frameworks"	D
C2	"heterogeneous artifact formats that impede consistent acquisition"	D
C3	"tamper-evident evidence preservation and verifiable custody records"	D
A1	"rapid evidence decay due to limited on-device storage"	D
A2	"auditable custody" and "transparent custody records"	I
A3	"verifiable custody records" with "blockchain-anchored time-ordering"	D
CR1	"a triad of persistent challenges"	NE
CR2	"sub-second anchoring latency under moderate load, linear scaling"	I
CR3	" Replay attempts are detectable via ledger uniqueness constraints and timestamp validation."	I

B.7 S7 – Zehra, Javed, Hyder, Darakhshan and Tariq (2024)

Table B7
Evidence extraction for S7: Zehra, Javed, Hyder, Darakhshan and Tariq (2024)

Req.	Evidence	Code
C1	" When a patient accesses his record using the “get record" function, he will have fake and incorrect reports or other doctor prescriptions"	I
C2	"available only for a public blockchain and are also proprietary"	I
C3	"the auditing and forensics process on logs collected through the smart contract"	I
A1	"we created a test bed in the form of a geth node so that we can collect logs and then analyze them ... our main purpose is to identify the forensic readiness on the blockchain"	D
A2	The give-access feature restricts access to a registered doctor when the modifier is present; architecture distinguishes patient, doctor and owner accounts. Found in "Figure 1: The architecture of EHR"	I
A3	"the mining node [Node3], whichmines the blocks. The other two are victim [Node2] andattacker [Node1] nodes, respectively. The miner nodetakes pending transactions from the transaction pool andverifies them. In order to impersonate the owner and doc-tor, we created two new accounts on Node3 while thepatient account is on Node2. Node2 has http.corsdomain“*” and allow-unsecure-unlock enabled which makes it atrisk."	D
CR1	"introduced some vulnerabilities into both theEHR smart contract and runtime environment of the geth node so that we can collect logs and then analyze them."	I
CR2	No continuity, backup, availability or recovery content appears in the study	NE
CR3	"After carrying out the attacks, wehave to analyze the transaction logs. For this purpose,we analyzed a lot of blockchain explorer tools"	I

B.8 S8 – Kyaw, Cusack and Lutui (2019)

Table B8
Evidence extraction for S8: Kyaw, Cusack and Lutui (2019)

Req.	Evidence	Code
C1	"flaws in wireless security encryption methods - WEP, WPA or WPA2. Accordingly, such vulnerabilities can be exploited and result in compromising the confidentiality, integrity, and availability of the organisation's data and information assets."	I
C2	"ISO/IEC 27043 highlights DFR as processes that focuses on pre-incident investigation" "be easily implemented and integrated into existing wireless networks in the healthcare sector"	D
C3	"file integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response" "to check the integrity of the patient's database. Any change in patient-related data will be logged"	D
A1	"forward them to a centralised logging system in order to preserve digital forensic evidence"	D
A2	"A Forensic readiness plan can help organisations not only to fulfil compliance requirements, but also to provide potential evidence during a DFI"	NE
A3	"controls devices and user's authentication based on the username and password"	D
CR1	"suitable for security risk coverage"	I
CR2	"is concerned with disaster recovery and business continuity ... However, the impact can also be minimised by having a digital forensic readiness (DFR) mechanism in place"	I
CR3	"real-time alerting and active response" "written to perform actions responding to security alerts"	D

B.9 S9 – Kyaw, Tian and Cusack (2020)

Table B9
Evidence extraction for S9: Kyaw, Tian and Cusack (2020)

Req.	Evidence	Code
C1	"The main purpose of a RADIUS server is to provide the authentication service for user's network connection requests and return appropriate configuration information, accordingly"	I
C2	"can be easily implemented and integrated into existing IoT and wireless networks in the healthcare sector"	D
C3	"provides extensive features such as file integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response … used to check the integrity of the patient's database. Any change in patient-related data will be logged"	D
A1	"all the users' activities (e.g. user success and failure logins, setting changes, and timestamp)"	D
A2	"as an integral component of an information security"	NE
A3	"RADIUS controls devices and user's authentication based on the username and password stored on the Domain Controller server. In this proposed DFR Framework, all the information and log (including username, timestamp, client MAC address) of the RADIUS server will be forwarded to the Syslog server as soon as a wireless client is successfully or unsuccessfully connected to the legitimate AP."	D
CR1	"mitigating security vulnerability in IoT medical devices by inserting forensic readiness states into the network system and preparing mitigation for security failure"	I
CR2	"can be easily implemented and integratedlxd to existing wireless networks in the healthcare sector."	I
CR3	"real-time alerting and active response"	D

B.10 S10 – Cusack and Kyaw (2012)

Table B10
Evidence extraction for S10: Cusack and Kyaw (2012)

Req.	Evidence	Code
C1	"influence can be exerted onto privacy security and control security"	I
C2	"The wireless connection of a human's most personal information is made into the medical information system that may extend beyond the immediate geographic location and access data storage facilities anywhere in a cloud network deployment. Similarly the hospital information system provides a push capability where the human vital statistics are controlled by feedback loops through the IT sensory systems. In both instances of push and pull, information risks to privacy and risks to life are exposed by the nature of the technology itself."	I
C3	"can track, trap and forward packets to the forensic server" "the cost of information storage is balanced against the benefit of having the evidence"	I
A1	"The system architecture is enhanced by adding a forensic server to the hospital information system and also the deployment of drones within the wireless network. Drones are not visible to the wireless network users but they can track, trap and forward packets to the forensic server"	D
A2	"Medical systems are designed for a range of end users in different professional skill groups"	NE
A3	"monitored by readers (fixed & mobile) and audited by mapping onto expected behaviours in the forensic server"	I
CR1	"The necessity of forensic readiness is a prudent risk treatment for such information systems"	I
CR2	"The utility cost to the service system is minimal as the forensic element is independent and self resourcing, and can function without visibility"	D
CR3	"A forensically ready system has security for prevention of events and forensic capability to investigate post events"	I

B.11 S11 – Gombar, Možnik and Pejić Bach (2026)

Table B11
Evidence extraction for S11: Gombar, Možnik and Pejić Bach (2026)

Req.	Evidence	Code
C1	"Embedded privacy safeguards; Compliance audit trails; Algorithmic accountability mechanisms"	D
C2	"anomaly detection relied on NIST intrusion-detection standards"	I
C3	"Proactive logging; Evidence preservation protocols; Cross-layer traceability"	D
A1	"Proactive logging; Evidence preservation protocols"	D
A2	"Compliance audit trails; Algorithmic accountability mechanisms"	D
A3	"Cross-layer traceability"	D
CR1	"Adaptive risk thresholds"	I
CR2	"the capacity of digital infrastructures to integrate forensic readiness with resilience mechanisms to ensure both anomaly detection and adaptive recovery"	D
CR3	"adaptive recovery refers to the capability of an infrastructure not only to restore functionality after disruption, but to iteratively improve recovery strategies based on forensic learning from prior incidents … evidence-informed and feeds back into detection thresholds, response prioritization, and resilience planning"	D

B.12 S12 – Mekala, Baig, Anwar, Syed and Zeadally (2025)

Table B12
Evidence extraction for S12: Mekala, Baig, Anwar, Syed and Zeadally (2025)

Req.	Evidence	Code
C1	"strict adherence to compliance and legal requirements in data handling"	I
C2	"based on the established Purdue model for ICSs"	D
C3	"A chain-of-custody protocol is established to ensure the integrity and admissibility of data" "securely transferred to centralized storage, with hash values generated to verify data integrity"	D
A1	"Data collection and preservation benefit from high automation, utilizing Security Information and Event Management (SIEM) systems like Snort/Intrusion Detection System (IDS) and Splunk for continuous monitoring" "Secure logging mechanisms capture Modbus TCP communications between SCADA and PLCs"	D
A2	"Policies and procedures are developed to address these threats, with clear roles assigned to IT security teams, plant operators, and forensic investigators"	D
A3	"forensic analysts leverage network and system logs to trace event sequences … Correlating such data helps to construct a comprehensive attack timeline"	D
CR1	"a comprehensive assessment of potential threats to and vulnerabilities of the IIoT architecture"	D
CR2	"the forensic process in the IIoT must prioritize the integrity and availability of data"	I
CR3	"to detect the attack source and the extent of its implications"	I

B.13 S13 – Adel, Ahsan and Davison (2024)

Table B13
Evidence extraction for S13: Adel, Ahsan and Davison (2024)

Req.	Evidence	Code
C1	"The use of privacy-enhancing technologies (PETs) during the identification phase of forensic investigations helps minimize the exposure of non-relevant personal data ... protecting the privacy of individuals not directly related to the case"	D
C2	"aims to streamline forensic processes while adhering to ethical standards"; "a standardized, universally accepted method for conducting digital forensics investigations"	I
C3	"gathering, extracting, preserving, and storing digital information" "Relevant ethical principles highlight the need to exclude data irrelevant to the investigation from reports to maintain focus and integrity. This exclusion helps prevent the dilution of forensic findings and reduces the risk of privacy violations"	D
A1	No logging, audit trail or monitoring mechanism is described among the eight roles or the framework layers	NE
A2	"establishes eight separate positions and their obligations in a digital forensics' investigation"; "The case handler is the orchestrator and organiser of the whole digital inquiry"	D
A3	"must also rebuild the defence's chronology using the retrieved data"	I
CR1	"Implementing standardized procedures and peer reviews can help mitigate the risk of bias"	I
CR2	"Digital forensic investigations can be resource-intensive ... Many organizations, particularly smaller ones, may lack the necessary resources ... This can lead to delays in evidence processing and analysis"	I
CR3	"eight different types of individual investigators."	I

B.14 S14 – Bankole, Taiwo and Claims (2022)

Table B14
Evidence extraction for S14: Bankole, Taiwo and Claims (2022)

Req.	Evidence	Code
C1	"ensures that judicial, regulatory and other laws within the organisation's realm of operation are considered and incorporated in the overall DFR strategy" "the implication of collecting private information [did not] emerge"	I
C2	"ensures that underlying policies and procedures are implemented according to agreed standards" "should strive towards ISO17025 certification"	D
C3	"which may include preserving the chain of custody, due-diligence, authenticity and relevance"	D
A1	"Cost/benefit analysis and a needs analysis for Monitoring tools" "How IDS triggers should function and respond" "Audit reports that measure conformance to governance requirements"	D
A2	"organisation structure depicting the forensic unit and responsibilities" "there should be a clear and explicit separation of responsibilities. Investigations should not be approved by the same group that is performing them"	D
A3	"identification and classification of source systems" "identification of business events"	I
CR1	"ensures the identification and classification of hardware, software, processes and events that house potential digital evidence. This is essentially a risk assessment that is conducted at business level"	D
CR2	"A cost/benefit analysis must be done before an investigation is commenced in order to determine the feasibility of such an investigation"	NE
CR3	"compile DF Incident report requirements … and have an incident escalation policy"	D

B.15 S15 – Janjua, Shah, Almogren, Khattak, Maple and Din (2020)

Table B15
Evidence extraction for S15: Janjua, Shah, Almogren, Khattak, Maple and Din (2020)

Req.	Evidence	Code
C1	"considers the security and privacy-aware distributed edge node log preservation by tackling the multi-stakeholder issue"; "For secure storage and session establishment for logs validation, Paillier Homomorphic Encryption, and SSL with Curve25519 is used"	D
C2	Named technologies used throughout: Holochain, Docker containerisation, Paillier Homomorphic Encryption, SSL with Curve25519, deployed on ARM-based architectures	I
C3	"We used Holochain to preserve log integrity, provenance, log verifiability, trust admissibility, and ownership non-repudiation"; features include "Proof of past log (PPL) preservation at fog level"	D
A1	"We propose an architecture for continuous log collection and preservation for IoT devices in a fog enabled cloud environment" "autonomous log collection"; Layer 1 dedicated to log generation and collection	D
A2	"the multi-stakeholder collusion problem … via assuring ownership non-repudiation and trust admissibility"	I
A3	"provenance … and ownership non-repudiation" "ownership non-repudiation and trust admissibility"	D
CR1	"adversarial model assumptions, security features, and limitations"	NE
CR2	"the automatic log harvesting running in containers gives a 95% confidence interval"	I
CR3	"none of the digital assets can be retrieved for forensics reincarnation"	I

C Evidence matrix and distribution summary

Table C1
Evidence for healthcare-sector requirements across the included studies

ID	Study	C1	C2	C3	A1	A2	A3	CR1	CR2	CR3	Direct
S1	Chernyshev et al. (2019)	I	D	D	D	I	D	I	I	I	4
S2	Grispos et al. (2017)	D	D	D	D	D	I	D	D	D	8
S3	Yaqub et al. (2026)	D	I	D	D	D	D	I	D	I	6
S4	Mpungu et al. (2024)	D	D	D	D	D	D	D	D	D	9
S5	Mishra & Bagade (2022)	I	I	D	D	NE	D	D	I	I	4
S6	Al-Balasmeh (2026)	D	D	D	D	I	D	NE	I	I	5
S7	Zehra et al. (2024)	I	I	I	D	I	D	I	NE	I	2
S8	Kyaw et al. (2019)	I	D	D	D	NE	D	I	I	D	5
S9	Kyaw et al. (2020)	I	D	D	D	NE	D	I	I	D	5
S10	Cusack & Kyaw (2012)	I	I	I	D	NE	I	I	D	I	2
S11	Gombar et al. (2026)	D	I	D	D	D	D	I	D	D	7
S12	Mekala et al. (2025)	I	D	D	D	D	D	D	I	I	6
S13	Adel et al. (2024)	D	I	D	NE	D	I	I	I	I	3
S14	Bankole et al. (2022)	I	D	D	D	D	I	D	NE	D	6
S15	Janjua et al. (2020)	D	I	D	D	I	D	NE	I	I	4
	Direct	7	8	13	14	7	11	5	5	6	76
	Indirect	8	7	2	0	4	4	8	8	9	50
	Not evidenced	0	0	0	1	4	0	2	2	0	9

Note. D = direct evidence; I = indirect evidence; NE = not evidenced in the reviewed article. C1 = data protection and privacy; C2 = interoperability and technical standards; C3 = evidence preservation and data minimisation; A1 = logging and monitoring; A2 = responsibility and governance; A3 = traceability and identification; CR1 = risk management; CR2 = operational continuity and preparedness; CR3 = incident response and recovery. Each code is supported by an entry in Appendix B giving the evidence and the assigned code.

Table C2

Distribution of evidence by dimension

Dimension	Direct	Indirect	Not evidenced	% Direct
Compliance (C1–C3)	28	17	0	62.2
Accountability (A1–A3)	32	8	5	71.1
Cyber resilience (CR1–CR3)	16	25	4	35.6
Total	76	50	9	56.3