Compliant Cyber Threat Intelligence Sharing in Hospitals: Evaluating the Data Anonymisation Tool

Ilkka Tikanmäki[1,2]1, Ammar Alhamada[1], James Lukins[1], Retina Nerjovaj[1], Marco Pastore[1] and Lauri Pöllänen[1]

[1]Laurea University of Applied Sciences, Espoo, Finland
[2]National Defence University, Helsinki, Finland

Ilkka.tikanmaki@laurea.fi

Abstract: Healthcare organisations face an unprecedented surge of cyberattacks targeting patient data, clinical systems, and connected medical devices. This study examines two ransomware and data breach cases in the United Kingdom and Finland over the past eight years. Both incidents reveal common weaknesses that could have been mitigated through robust Cyber Threat Intelligence (CTI). Despite its benefits, CTI sharing among hospitals remains rare due to privacy concerns, fear of regulatory violations, and limited institutional trust. Under the General Data Protection Regulation (GDPR) and the emerging EU Cyber Resilience Act (CRA), CTI often includes personal or sensitive system data requiring strict protection and traceability, creating tension between collaboration and compliance. This research evaluates whether the Data Anonymisation Tool (DAT) can enable secure, auditable, and GDPR-compliant CTI sharing. The methodology combines a systematic literature review, regulatory mapping of GDPR and CRA obligations, and a functional assessment of DAT's anonymisation and audit capabilities. Simulated CTI-sharing scenarios test how anonymised threat data can flow between healthcare organisations without exposing identifiable information. Findings indicate that DAT integrates technical, legal, and governance safeguards into a single process. It delivers GDPR-compliant anonymisation, preserves CTI utility, and ensures full traceability through verifiable audit logs, addressing CRA requirements for accountability and resilience. While governance challenges persist, particularly around trust models and sector-specific standards, DAT demonstrates strong potential to transform compliance barriers into enablers of collaboration. Privacy-preserving CTI sharing is feasible when supported by structured anonymisation and auditing mechanisms. DAT offers a viable pathway to enhance healthcare cyber resilience and aligns with European efforts to promote secure data sharing in critical sectors.

Keywords: Cyber Threat Intelligence (CTI), Data anonymisation, Cyber Resilience Act (CRA), Healthcare cybersecurity, Privacy-preserving collaboration

1. Introduction

Cyberattacks targeting the Healthcare sector have increased significantly over the past decade, affecting hospitals, clinics, laboratories, and medical device networks. Ransomware, phishing, and exploitation of vulnerabilities in Internet of Medical Things (IoMT) systems routinely disrupt clinical operations and compromise patient safety. Cyber Threat Intelligence (CTI) sharing has emerged as a critical capability for strengthening collective cyber defence. By exchanging information on indicators of compromise, attack patterns, and emerging threats, hospitals could detect incidents earlier and respond more effectively.

Hospitals often refrain from collaborating due to concerns about privacy, data sensitivity, and regulatory compliance, especially under the General Data Protection Regulation (GDPR) and the recently introduced Cyber Resilience Act (CRA). CTI datasets frequently contain personal or system-identifying information that must be protected, traceable, and processed according to strict legal requirements. Real-world incidents analysed in this study, specifically ransomware and data breach cases in the United Kingdom and Finland, illustrate how insufficient patching practices and the absence of CTI sharing amplify the operational and security impacts faced by healthcare organisations.

Hospitals lack a clear and compliant mechanism for exchanging incident information without risking exposure of sensitive data. This research addresses that gap by focusing on the potential of the Data Anonymisation Tool (DAT) to enable secure and regulation-aligned CTI sharing under the EU's evolving cybersecurity framework.

The research question of this study is:

- How can the DAT support secure and compliant CTI sharing among hospitals under the EU CRA?

The rest of the paper is organised into four chapters. Chapter 2 presents a literature review pertinent to this study and outlines the document's scope. Chapter 3 offers both theoretical and practical backgrounds. Chapter 4 outlines the findings, and Chapter 5 provides the conclusions of the study.

[1]https://orcid.org/0000- 0001-8950-5221

2. Literature

The increasing complexity of cyber threats in the healthcare sector has generated a growing interest in cyber threat intelligence (CTI) sharing as a collective defence mechanism (Fischer, 2023). Research consistently shows that CTI sharing faces substantial barriers. (Skopik et al., 2016) highlight issues of low inter-organisational trust, fragmented governance structures, and unclear responsibilities regarding incident information exchange. A key barrier identified in the literature concerns the sensitivity and identifiability embedded in CTI datasets. (Weber et al., 2023) demonstrate that log files, indicators of compromise, and incident reports often contain personal data, system configuration details, or operational metadata that can reveal internal processes. Organisations operating under GDPR face pressure to ensure that any transferred data remains compliant, minimising the risk of unlawful disclosure (Casarosa, 2023).

(Gadotti et al., 2024) show that anonymisation can enable privacy-preserving collaboration but emphasise the absence of standardised approaches tailored to specific domains such as healthcare. Existing tools such as ARX, Amnesia, and various pseudonymization frameworks provide partial solutions but frequently lack auditability, sector-specific configuration, or full alignment with regulatory principles such as accountability, data protection by design, and secure processing.

The regulatory landscape further complicates CTI sharing. Under GDPR, personal data must be processed lawfully, transparently, and with minimisation principles. CRA places additional obligations on organisations managing digital products and services, demanding traceability, security-by-design, and demonstrable accountability across the product lifecycle (European Parliament and of the Council, 2024). The coexistence of GDPR and CRA creates uncertainty for organisations regarding how to share operational security data while maintaining compliance.

The Horizon Europe DYNAMO project proposes an integrated approach that combines CTI, Business Continuity Management (BCM), and data anonymisation processes (DYNAMO project, 2024; Tikanmäki et al., 2025). The Data Anonymisation Tool (DAT) is designed to support compliant CTI exchange by embedding technical anonymisation, governance controls, and audit features within a single framework. Academic analysis of such tools remains limited, and few studies examine their alignment with emerging EU regulatory expectations.

3. Method

This study employed a multi-stage methodology combining a systematic literature review, regulatory mapping, functional analysis, and scenario-based evaluation of the Data Anonymisation Tool (DAT). The aim was to determine whether DAT can support secure and compliant CTI sharing under GDPR and the EU Cyber Resilience Act (CRA).

A systematic literature review was conducted using academic databases and policy repositories. Twelve key sources published between 2016 and 2024 were selected based on relevance to three thematic areas: CTI sharing barriers and trust challenges; anonymisation techniques and privacy-enhancing technologies; and EU regulatory frameworks shaping cybersecurity and data protection obligations. A regulatory mapping analysis was performed to evaluate how DAT aligns with GDPR and CRA principles. GDPR mandates data protection by design, secure processing, and appropriate technical safeguards. A functional assessment of DAT was conducted to analyse its anonymisation workflow, audit-trail mechanisms, and integration within DYNAMO's combined CTI and Business Continuity Management (BCM) framework (DYNAMO project, 2023). Simulated CTI-sharing scenarios were examined to assess how anonymised incident data could be exchanged between healthcare organisations while preserving analytical value.

The methodology included a brief analysis of two real-world healthcare cyber incidents: a major ransomware attack affecting hospital services in the United Kingdom (The National Audit Office, 2018) and a large-scale patient data breach in Finland (Office of the Data Protection Ombudsman, 2021). These cases were selected due to their public documentation and relevance to CTI failures. Case studies served to contextualise how CTI sharing, if supported by anonymisation and compliance mechanisms, could have reduced the severity or impact of these attacks.

4. Results

The analysis identifies the regulatory, organisational, and trust-related barriers (Bak et al., 2023) that currently limit CTI sharing across healthcare organisations. The evaluation examines how the DAT addresses these barriers through its anonymisation workflow, governance controls, and audit-trail mechanisms. The research assesses

DAT's alignment with GDPR and CRA requirements and evaluates its performance in simulated CTI-sharing scenarios to determine whether anonymised threat intelligence remains operationally useful. These findings provide a comprehensive understanding of both the challenges faced by hospitals and the potential of DAT to support compliant and privacy-preserving CTI collaboration.

Healthcare organisations face systemic cybersecurity risks, yet CTI sharing remains uncommon due to regulatory uncertainty, data sensitivity, and limited institutional trust. CTI logs often contain identifiable information, creating ambiguity about lawful processing under GDPR. Existing anonymisation tools lack sector-specific guides and audit trails, preventing hospitals from demonstrating compliance. These findings highlight the need for a unified tool that can operationalise privacy and accountability.

In both the UK and Finnish incidents, attackers exploited unpatched systems and weak security monitoring capabilities, demonstrating the operational consequences of insufficient CTI utilisation. Relevant threat indicators had been observed in other regions before the attack, but were not shared or acted upon locally due to regulatory uncertainty, negligence and limited trust between organisations.

DAT integrates anonymisation and audit logging within DYNAMO's combined CTI and BCM ecosystem. DAT removes sensitive attributes while preserving operational utility and generates verifiable audit logs that support accountability and regulatory compliance. This operationalises GDPR and CRA principles directly into the CTI workflow, converting compliance requirements into enablers of collaboration.

Simulated CTI-sharing scenarios confirmed that anonymised data retained its analytical value. Mapping DAT's processes to GDPR and CRA requirements demonstrated strong alignment with data protection by design, secure processing, and traceability expectations. Remaining challenges relate to governance models, trust frameworks, and sector-specific standardisation, suggesting paths for future refinement.

5. Discussion and Conclusions

The findings demonstrate that DAT offers a viable and practical approach to privacy-preserving CTI sharing. By integrating technical, legal, and organisational safeguards, the tool directly addresses the core barriers preventing healthcare organisations from collaborating. The study also supports EU policy objectives such as those in the CRA and the European Health Data Space by providing evidence of how regulatory principles can be transformed into operational mechanisms.

However, governance remains a critical factor. Adoption of DAT will require standardised CTI policies, sector-wide trust frameworks, and training to support consistent use. Although DAT provides strong technical and legal alignment, long-term success will depend on how well healthcare institutions embed these practices within their cybersecurity operations.

This study examined whether DAT could support secure and compliant CTI sharing among hospitals. The analysis shows that DAT effectively removes sensitive information, maintains analytical value, and ensures accountability through audit trails. Its alignment with GDPR and CRA principles demonstrates that privacy-preserving CTI sharing is feasible.

Future work should focus on real-world pilot testing, governance model development, and wider integration of DAT into healthcare cybersecurity practices. Despite remaining challenges, DAT represents a promising step toward collective cyber resilience in the healthcare sector.

Acknowledgements

This study has received funding from the European Union project DYNAMO, the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 101069601 and The Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Ethics declaration: No human participants or personally identifiable information were involved. All data sources were publicly available.

AI declaration: Keenious was used for literature exploration, and ChatGPT 5.1 for drafting and refinement. Human authors verified all content.

References

Bak, M. A. R., Ploem, M. C., Tan, H. L., Blom, M. T., & Willems, D. L. (2023). Towards trust-based governance of health data research. *Medicine, Health Care and Philosophy*, *26*(2), 185–200. https://doi.org/10.1007/s11019-022-10134-8

Casarosa, F. (2023). *Cybersecurity of Internet of Things in the Health Sector: Understanding the Applicable Legal Framework* (SSRN Scholarly Paper No. 4633584). Social Science Research Network. https://doi.org/10.2139/ssrn.4633584

DYNAMO project. (2023). *Factsheet 2: Cyber Threat Intelligence*. DYNAMO Project. https://horizon-dynamo.eu/wp-content/uploads/2023/09/DYNAMO-Factsheet-2-1.pdf

DYNAMO project. (2024). *D4.1 – Initial prototypes of the cyber-threat intelligence gathering, extraction, sharing components and AI-based solutions. [*. https://horizon-dynamo.eu/wp-content/uploads/2025/02/DYNAMO-RPT-D41-V2-0.pdf

European Parliament and of the Council. (2024, November 8). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future*. European Parliament. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Parliament and the Council. (2016, April 27). *General Data Protection Regulation (GDPR)*. European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504

Fischer, B. (2023). *Privacy-Preserving Federated Learning for Cyber Threat Intelligence Sharing* [Master Thesis, Swiss Federal Institute of Technology]. https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/appliedcrypto/education/theses/MSc-Thesis-Benjamin-Fischer.pdf

Gadotti, A., Rocher, L., Houssiau, F., & Creţu, A.-M. (2024). Anonymization: The imperfect science of using data while preserving privacy. *Science Advances*, *10*(29), 22. https://doi.org/10.1126/sciadv.adn7053

Office of the Data Protection Ombudsman. (2021). *Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations* [Press Release]. Administrative Fine Imposed on Psychotherapy Centre Vastaamo for Data Protection Violations. https://tietosuoja.fi/en/-/administrative-fine-imposed-on-psychotherapy-centre-vastaamo-for-data-protection-violations

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

The National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS* (Investigation No. HC 414; p. 35). National Audit Office. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf?utm_source=chatgpt.com

Tikanmäki, I., Rajamäki, J., Johnston, E., Salenius, J., Teräväinen, J., Tuovila, P., Feiring, P., Sissonen, M., Winberg, A., & Ybañez, K. (2025). DYNAMO and the EU AI Act: Balancing Innovation and Regulation. *International Conference on Cyber Warfare and Security*, *20*(1), Article 1. https://doi.org/10.34190/iccws.20.1.3307

Weber, S., Stein, S., Pilgermann, M., & Schrader, T. (2023). Attack Detection for Medical Cyber-Physical Systems—A Systematic Literature Review. *IEEE Access*, *PP*(99), 1–1. https://doi.org/10.1109/ACCESS.2023.3270225