doi: 10.37394/23205.2024.23.1

Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals

JYRI RAJAMÄKI, DOMINIK JARZEMSKI, JIRI KUCERA, VILLE NYMAN, ILMARI PURA, JARNO VIRTANEN, MINNA HERLEVI AND LAURA KARLSSON
Unit W,
Laurea University of Applied Sciences,
Vanha maantie 9, 02650 Espoo,
FINLAND

Abstract: - The DYNAMO Horizon Europe Project aims to support critical sector (healthcare, energy production, marine transport) stakeholders in enhancing resilience and minimizing the effects of cyber-attacks. DYNAMO's objective is to use artificial intelligence to integrate cyber threat intelligence (CTI) and business continuity management (BCM) to support decision-making. The goal is joint preparation for EU cyber threats, necessitating timely global situational awareness and effective communication to address threats before they escalate. This paper focuses on the intelligence sharing and trust needs of the DYNAMO use cases while also meeting regulatory requirements. Analyzing DYNAMO's internal materials and aligning them with authorities' requirements, particularly NIS2 and GDPR, reveals that healthcare organizations need to prepare for more effective data protection, incident response, and cyber-attack mitigation. While NIS2 doesn't specify technical requirements for healthcare, it offers a broader framework for organizations to make informed decisions about equipment suppliers and security applications. After the general review, this study examines a specific healthcare use case: a hospital infected by phishing, emphasizing that CTI exchanges may contain sensitive data falling under GDPR and NIS2 regulations. This includes technical details, health-related information, patient data, insurance details, and employee information. Concerning the AI-based approaches used, DYNAMO must handle this CTI exchange in compliance with the law. The case study compares the DYNAMO project's CTI exchange use case with GDPR and NIS2 requirements, highlighting challenges such as the difficulty in separating sensitive data under GDPR and differences in language and terms between the two regulations. Despite these challenges, the study discusses the impact of GDPR and NIS2 on CTI exchange in the healthcare sector, providing key implementation points and guidelines.

Key-Words: - Cyber threat intelligence, Critical information infrastructure protection, CTI exchange, Cyber security in hospitals, NIS2, GDPR, Dynamo project.

Received: August 8, 2023. Revised: December 2, 2023. Accepted: February 9, 2024. Published: April 1, 2024.

1 Introduction

The use of digital technologies and electronic health Advancements in technology have made it so that the cyber threat surface of the healthcare sector is exponentially larger now than it was even 20 years ago. For example, patient records are saved in a digital format and many wired and wireless medical devices are part of the Internet of Medical Things, [1]. These are just two examples of many, but they both present opportunities for cybercriminals. Gaining access to a hospital network can become very profitable for adversaries through ransomware, or accessing systems related to Electronic Medical Records (EMR). There are also threats to patient safety that are related to making network-connected medical equipment malfunction. Although the benefits of these systems and tools far outweigh the negatives, they have made it difficult for healthcare facilities to protect themselves against all possible threats lurking in the shadows of the internet. One big question is how a single hospital can defend itself. Unfortunately, there is not a single answer, but improved cybersecurity policies can point the way to a more secure future, [2].

The DYNAMO Horizon Europe Project aims to support critical sector (healthcare, energy production, marine transport) stakeholders in enhancing resilience and minimizing the effects of cyber-attacks. DYNAMO aims to increase digitalization in the current context of increased cyber threats through the DYNAMO platform which uses artificial intelligence to integrate cyber threat intelligence (CTI) and business continuity

management (BCM) to support decision-making. The goal is joint preparation for EU cyber threats, necessitating timely global situational awareness and effective communication to address threats before they escalate, [3].

Healthcare is classified as a critical industry. Implementation of the new Network and Information Security (NIS2) Directive is still in progress, but the deadline for compliance is fast approaching, [4]. Nor has the impact of the General Data Protection Regulation (GDPR) on CTI exchange been studied. While NIS2 doesn't specify technical requirements for healthcare, it offers a broader framework for organizations to make informed decisions about equipment suppliers and security applications. Health data is critical personal data that is specifically regulated by the GDPR.

This study focuses on intelligence sharing and trust needs of the DYNAMO use cases while also meeting regulatory requirements. The main goal of the paper is to find out how the implementation of NIS2 is going to affect CTI sharing. Analyzing DYNAMO's internal materials and aligning them with authorities' requirements, particularly NIS2 and GDPR, reveals that healthcare organizations need to prepare for more effective data protection, incident response, and cyber-attack mitigation. It is important to state that such CTI exchange could contain data relevant to GDPR and NIS2 legislations. To ensure the longevity and trust of DYNAMO solutions, DYNAMO must be compliant with the regulations, which is the main motivation behind this paper. This paper will specifically look at the scenario where hospitals become infected by phishing and the possible CTI exchange for such cases. The scenario covers the possibility of accessing the server farms, including the Aqure Database, LIS (Laboratory Information System), and SIO (Hospital Information System) through a smart worker's infected PC.

2 Cyber Threat Landscape in Hospitals

2.1 Current Cyber Threats Facing Healthcare Organizations

The healthcare industry is becoming digitalized as electronic services increase. Examples of these are electronic health records (EHR), medical Internet of Things devices, and telehealth solutions. However, with digitalization, hospitals are increasingly exposed to cyber security threats, and nowadays, the healthcare sector is the main target of cybercriminals, [5] and healthcare is considered one of the most targeted sectors for cyber security breaches, [6]. For example, in the 2020 cyberattack affecting the University of Vermont Health Network, the organization lost all network intranet services, clinical systems (including laboratory, pathology, pharmacy, and radiology systems), email communications, and their electronic medical record system, [7]. Table 1 lists current cybersecurity issues in hospitals and the healthcare industry.

2.2 Understanding Cyber Threat Intelligence Exchange

Cyber threat intelligence (CTI) can function as an important part of organizations' cyber security defenses. It is at its core almost a functional requirement to use intelligence to defend against cyber threats, [8]. This is highly related to the speed at which adversaries move. There is a constant race between attackers looking for weaknesses, and defenders improving their defenses and protecting their companies. Cyber threat intelligence comes into play here and provides defenders with vital information they can use to improve their defenses.

There are three main types of cyber threat intelligence: strategic, tactical, and operational. Starting with strategic threat intelligence is less technical and focuses on giving high-level threat intelligence that can be used to provide organizations with an overview of the threat landscape. This usually includes different kinds of reports and news. The primary target for this kind of threat intelligence is non-technical audiences, [9].

Tactical threat intelligence is very different from strategic, as it is aimed at technical audiences and focuses on Indicators of Compromise (IoCs). These include malicious domain names, URLs, IP addresses, and other malicious traffic. With the help of threat information, IT teams can reduce the organization's risks. By identifying various threats and reacting to them proactively, organizations can protect themselves from them by incorporating them into their information security practices, [9].

Operational Threat Intelligence is mainly aimed at people working in security operations centers. Such threat intelligence often provides an overview of how different threat actors plan and execute their attacks and operations. This includes understanding their tactics, techniques, and procedures. The main benefits of this type of threat intelligence are improved threat monitoring, management, and incident response, [9].

Table 1. Cybersecurity issues in hospitals and the healthcare industry

Cybersecurity issue	Manifestation in hospitals and the healthcare industry
Ransomware Threats	Hospitals stand as primary targets for ransomware attacks. Cybercriminals encrypt vital medical data and demand payment for its release, [10]
Patient Data Breaches	Because healthcare organizations store large amounts of sensitive patient data in electronic health records (EHRs), they are attractive targets for data breaches. As a result, identity theft, insurance fraud, and privacy violations, [11]
Outdated Systems	Many healthcare systems rely on legacy software and outdated operating systems. Therefore, they are vulnerable to exploitation due to the lack of up-to-date security fixes, [12]
Vulnerabilities in Medical Devices	The increasing connectivity of medical devices brings with it vulnerabilities that can be used to manipulate patient data, disrupt the operation of the device, or endanger patient safety, [13]
Insider Threat	Individuals with access to healthcare systems can pose threats through intentional or accidental actions. These include data theft, misuse of access rights, or unintentional disclosure of sensitive information, [14]
Cybersecurity Awareness Deficiency	Inadequate training and awareness of cybersecurity best practices among healthcare personnel: Potentially resulting in human error, such as falling victim to phishing attacks, [15]
Supply Chain Weaknesses	The complex supply chains of healthcare organizations are vulnerable to vulnerabilities in the cybersecurity measures of suppliers and third-party services. They allow attackers to infiltrate the hospital's network, [16]
Interconnected Healthcare Systems	The interconnected nature of the healthcare ecosystem: Multiple parties sharing patient data, creating numerous vulnerabilities to cyber threats, [17]
Regulatory Challenges	Healthcare organizations must comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA), [18]. However, for some, compliance and security were additional tasks added to already expected day jobs. For others, the confusion and complexity surrounding the process and expectations led to inaction, [19].
Financial Limitations	Many healthcare organizations face budget constraints and a shortage of skilled cybersecurity personnel, hindering the implementation of robust cybersecurity measures and timely responses to emerging threats, [20].

Machine-readable threat intelligence (MRTI) is information about cyber security threats and vulnerabilities that can be understood and processed by automated systems. Compared to manual kinds of cyber threat intelligence, MRTI allows for quicker and more automated threat detection, response, and mitigation. Utilized properly, it can help organizations enhance their ability to automate the detection and response to cyber security threats. This would allow for less security analyst manpower required to do the same amount of work. Related to this, automated systems can quickly ingest, analyze, and act upon threat intelligence, as there is no human input required, [21].

2.3 Benefits of Threat Intelligence Sharing in Healthcare

Most of the healthcare organizations carry some type of specialized hospital information system. Protection of these systems and devices is crucial and the healthcare sector utilizes cyber threat intelligence to strengthen its cybersecurity defenses, detect and respond to threats, and ensure compliance with industry regulations. The most common ways for cyber threat utilization are threat detection and prevention, incident response and mitigation, vulnerability management, ISAC participation, phishing, and social engineering defense, regulatory compliance, security awareness training and user education as well as vendor risk management.

While the benefits of digital systems and devices in healthcare are substantial, defending against cyber threats has become a complex challenge for hospitals. One crucial approach to support cybersecurity defenses is the utilization of CTI, which plays a vital role in providing organizations with essential information to enhance their security posture. The introduction of machine-readable threat intelligence (MRTI) enhances the efficiency of cybersecurity measures. MRTI allows for automated processing and integration into security policies. This promotes quicker and more automated threat detection, response, and mitigation, reducing the need for extensive security analyst manpower. The

integration of advanced technologies, such as MRTI, is crucial for building resilience against evolving cyber threats in the healthcare sector.

3 Regulatory Landscape for Healthcare Organizations

The European health industry must respond to the protection, safety and increasing well-being needs of an aging society, [22]. The pandemic situation further increased the urgency of the health industry, [23]. Digital technologies offer cost efficiency, additional capacity, and better user experiences of health services, [24]. Automation technologies used in industrial control systems or industrial automation control systems provide a crucial role in ensuring the availability of critical services in society, such as smart grid, water distribution, digital healthcare, etc., [25]. However, as technologies evolve, privacy and data protection frameworks must be in place to strike a balance between securing health information and encouraging innovation, [26].

3.1 Impact of GDPR on Cybersecurity Practices

GDPR is legislation that determines how personal data can be used by organizations and companies and how it can be processed (meaning e.g., collected, structured, organized, erased). GDPR defines personal data as any data that could identify a living person, including but not limited to contact information, health data, and online behavior. GDPR has the following implications for hospitals' cybersecurity practices:

- Data Protection Principles: GDPR emphasizes the protection of personal data. Hospitals must ensure that any data shared as part of cyber threat intelligence does not compromise patient privacy or violate GDPR principles.
- Lawful Basis for Processing: Hospitals must have a lawful basis for processing personal data. Consent, contractual necessity, legal obligations, vital interests, public tasks, and legitimate interests are some of the lawful bases. Hospitals need to determine the most appropriate basis for sharing threat intelligence.
- Data Minimization: GDPR requires organizations to collect and process only the minimum amount of personal data necessary for a specific purpose. Hospitals must apply the principle of data minimization when sharing threat intelligence to avoid unnecessary exposure to sensitive information.
- Security Measures: GDPR mandates that organizations implement appropriate security measures to protect personal data. Hospitals engaging in threat intelligence sharing must ensure that these measures are in place to safeguard the information exchanged.
- International Data Transfers: If a hospital shares threat intelligence internationally, GDPR's restrictions on cross-border data transfers must be considered. Adequate safeguards or legal mechanisms (such as Standard Contractual Clauses) may be necessary.

For this paper, within identified potential data, we see the connection to the “Personal data” and “Health-related data” categories. Certain technical data, such as IP addresses, could be connected to a certain person, meaning it also falls under GDPR law, [27]. To conduct a CTI exchange involving GDPR-protected data, it is only legal in case data is necessary and the legal groundwork for sharing can be labeled as a legitimate interest. Any remaining data must either be randomized or anonymized, [28]. In the context of CTI exchange due to hospitals being infected via phishing, this poses questions if all the data that could be provided is necessary, and whether its sharing can be linked with a legitimate interest.

3.2 NIS2 and Critical Information Infrastructure Protection

NIS2 sets out a cybersecurity regulatory framework, requiring European Union Member States to strengthen cybersecurity capabilities and risk-management measures, along with rules on cooperation and information sharing, [29]. NIS2 aims to achieve a high common level of cybersecurity across the member states. Member states do not share cybersecurity-related information systematically, leading to negative consequences in the effectiveness of the cybersecurity measures. NIS2 proposal had more detailed general objectives, one of which was to improve the level of joint situational awareness and the collective capability to prepare and respond. Directive entered into force on 16 January 2023 and member states now have time until 17 October 2024 to transpose its measures into national law, [30].

Complex environments and the amount of information that needs to be kept confidential can pose challenges to the effective sharing of CTI information. Also, limited resources within

healthcare organizations can complicate the implementation of directives like NIS2 into daily operations, [31]. The NIS2 directive provides measures to increase cybersecurity levels in the EU and expands the scope of the initial NIS directive into critical sectors, such as healthcare, [32]. As such, NIS2 will also apply to the defined scope of the CTI exchange, as the threat occurred in the healthcare sector. For this paper, NIS2 has at least the following effects:

- Critical Infrastructure Requirements: NIS2 focuses on enhancing the security of critical infrastructure, including healthcare. Hospitals are classified as operators of essential services (OES), and they must implement robust cybersecurity measures, including incident response and threat intelligence sharing capabilities.
- Incident Reporting Obligations: NIS2 imposes mandatory incident reporting requirements for OES, including hospitals. When a cybersecurity incident occurs, hospitals must report it to the relevant national authority and may need to share information about the incident.
- Collaboration and Cooperation: NIS2 encourages collaboration and cooperation between OES, including sharing threat intelligence, to strengthen overall cybersecurity resilience. However, the sharing must comply with data protection regulations such as GDPR.
- Security Measures and Standards: Hospitals are required to implement appropriate security measures and follow established cybersecurity standards. NIS2 emphasizes the importance of risk management and cybersecurity practices to protect against cyber threats.

The directive as such addresses the following security measures: risk analysis and information system security policies; incident response; business continuity and crisis management; supply chain security; effectiveness of risk management measures; encryption and vulnerability disclosure. From those areas, we have deduced that incident response, business continuity, and crisis management lie within the scope of this paper.

4 Case Study - Infection via a VPN Connection

4.1 Scenario Overview

The case study scenario is an attack on the hospital's server farm via a remote user's laptop attacking it via a VPN connection. The connection will attack the Aqure (SQL) system and through this the server farm. The attack via specific malware can be done remotely without the attacker being in the hospital premises.

An employee working remotely (teleworker) using his / her personal computer is connected to Aqure through a VPN to perform his / her tasks. The employee has received a phishing email with an infected attachment, which contains malware. The malware has propagated from the employee's device and via the VPN to Aqure. As a result, a malicious user can remotely enter the system and perform the attack. Hence, a system such as DYNAMO might have to install specific software tools in the two (2) firewalls which will send an indication to the hospital IT team. Actors involved in the scenario are the remote worker (who received an infected phishing email) and the malicious user (who can remotely enter the system and perform the attack).

To propagate ransomware, it is not necessary to disable the firewall if the firewall does not perform deep inspection of the packets. In this scenario, the external attacker must bypass the hospital firewalls. Hence, they can have access to the Aqure web server. Through Aqure, they can modify or even destroy the Aqure database. As a further step, the attacker will have access to the Laboratory Information System (LIS) and potentially disrupt its operations. The attacker may also target the Hospital Information System (SIO), which grants access to the hospital environment, enabling him/her to shut down hospital systems and force employees to revert to manual operations, which are very slow and completely prone to errors. All such access will happen if an unidentified user enters some software through a USB key to the point-of-care testing (POCT) machine.

The purpose of the DYNAMO platform and the software tools that work on it is that unusual operations are detected without delay, IT is informed, and the operation is stopped. Attacks are greatly reduced to create access points to the hospital server. For this scenario, a DYNAMO software tool will be installed in the POCT and/or the internal firewall which will detect unconventional operations and provide detection to the IT department and stop such operations. The

operation of the DYNAMO platform should make the POCT more reliable against possible attacks than it currently is, as currently it is running on Windows XP/7 and has no antivirus software present. DYNAMO aims to add such features to make attacks less likely to involve and create an entry point to the hospital server farm. In this scenario, care must also be taken that: (1) continuity of centralized POCT management via the Aqure system, (2) protection of the personal workstation of the smart worker, and (3) protection from the smart worker's workstation.

4.2 GDPR Landscape for the Scenario

Projects such as DYNAMO are recommended to prepare a Data Protection Impact Assessment due to the risk of GDPR breach of other's data. In this assessment, it is necessary to outline the risks to the rights and freedoms of individuals, justify the need for processing the data and its intended purpose, and include mechanisms to ensure the protection of personal data while including the legitimate interest, [33]. It is important to point out that such an assessment does not have a set format – while it is possible to find recommended templates, this is an area that is somewhat complicated for the person implementing this legislation. Hence, for the DYNAMO project, it would be important to figure out what the format of such an assessment would be and what data would be included in the CTI exchange. On the contrary, one of the primary advantages of implementing GDPR controls is that while the main objective is achieving legal compliance, the project will also enhance control over patients' personal information, thereby providing an ethical benefit.

To ensure compliance during CTI exchanges, DYNAMO should anonymize identifiable data like personal and health information. This involves monitoring outgoing data closely and applying anonymization techniques effectively. This will also require proper tooling to ensure anonymization can be achieved.

In the above scenario, the attacker accesses or uses the smart worker's machine, the laboratory information system, and the hospital information system. In this case, it can be assumed that the following data containing personal data may be used in the CTI exchange:

- Technical data – e.g., IP addresses, hardware specification, network architecture
- Health-related data – e.g., test results, details of medical conditions
- Personal data – e.g., name and surname of patients and hospital workers, insurance information

4.3 NIS2 Landscape for the Scenario

NIS2 directive covers a range of critical industries, that are considered sectors of high criticality and are essential to have a high level of security measures, one of which is the health, and healthcare providers, sector which was already regulated in the original NIS directive. The obligations are further regulated by national legislation, but NIS2 sets out the baseline for cybersecurity risk-management measures and reporting obligations in critical industries.

NIS2 overlaps in many ways with CTI sharing. Article 7 introduces guidance for the national cybersecurity strategy that shall include among other objectives:

- an identification of the measures ensuring preparedness for, responsiveness to, and recovery from incidents, including cooperation between the public and private sectors
- managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12
- including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities by Union law.

In Article 12 there are measures set for coordinated vulnerability disclosure. Having a national-level CSIRT (Computer Security Incident Response Team) responsible for coordinating for example measures, such as assisting legal entities in reporting vulnerabilities. The whole Chapter III of NIS2 is dedicated to cooperation at the union and international level.

Article 21 consists of Cybersecurity risk-management measures. This article aims to set measures that protect network and information systems and the physical environment of those systems from incidents. Article 20 sets requirements for Member States to ensure that all affected entities approve the cybersecurity risk-management measures in Article 21. In terms of CTI sharing, the main measures in Article 21 include:

- Risk analysis and information system security policies
- Incident handling
- Business continuity
- Supply chain security

- Security in network and information systems acquisition, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and encryption
- Use of multi-factor authentication and secured communication systems within the entity, where appropriate.

Article 23 consists of reporting obligations. Member state shall ensure that when significant incidents occur; meaning it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage, there must be measures to ensure that notifications of these incidents will be done without undue delay to CSIRT or the competent authority to determine any cross-border impact of the incident.

The two timeframes specified in Article 23 are 24 and 72 hours. An early warning must be provided promptly, within 24 hours of discovering a significant incident. This warning should indicate whether the incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact. In 72 hours, an initial assessment of the significant incident must be given, including severity and impact assessment of the incident, as well as the indicators of compromise, if available.

Article 24 introduces the possibility for Member States to set requirements to use ICT services and ICT processes that are certified under European cybersecurity certification schemes. CTI systems should therefore be developed, in a way that they can be accredited and certified if obligated. In NIS2, administrative fines are introduced. Articles to be enforced and have penalties for infringing them include articles 21 and 23.

Examining the scenario in the context of NIS2 compliance, it can be concluded that NIS2 has a couple of articles specifically that cover the scenario. Articles 7, 12, 21, and 23 that were covered previously. They pertain to a broad set of requirements for management, training, and technical tools for security in general. NIS2 does not go to specific demands, such that every hospital needs to have an IPS or IDS in their network. It's a broader set of requirements that could be achieved partly by installing an IPS/IDS system. These technical details are left to the organization to decide upon themselves to achieve compliance with the NIS2 directive. The examined scenarios are subject to the mandatory incident reporting regime established by the NIS2 directive. This directive, building on the former NIS directive, mandates that actions must be taken towards the national CSIRT within 24 hours of becoming aware of the incident, with sanctions for non-compliance, [29]. The extent to which information should and can be shared has to be assessed by the notifier so that the notification fills the requirement of NIS2 while still complying with other regulations such as GDPR, [34].

5 Discussion

The General Data Protection Regulation (GDPR) and the Network and Information Systems Directive 2 (NIS2) are European regulations that have significant implications for cybersecurity practices, including cyber threat intelligence sharing. Hospitals must strike a balance between cybersecurity collaboration, legal compliance, and patient data protection when engaging in cyber threat intelligence sharing. Regular updates on relevant regulations and collaboration with legal and cybersecurity experts are crucial for maintaining a robust and compliant approach.

As a result of examining the scenario, it is found that GDPR poses challenges for the implementation of the DYNAMO platform because some CTI materials contain information that can be classified as personal data. Instead, the NIS2 Directive is a good basis for DYNAMO. As the purpose of this legislation is to implement better control of cyber security incidents in relevant industries [32] as in this case healthcare, the idea of the DYNAMO project is in line with this goal.

The DYNAMO platform and tools have functions that support the successful implementation of the NIS2 directive. First, as mentioned above, DYNAMO improves such response by sharing this information with other relevant targets and ensuring hardened systems against a future attack. Secondly, in terms of business continuity and crisis management, DYNAMO includes parts that are relevant, such as hardening systems and ensuring risk assessment, [3]. All these factors, including staff training, contribute to successfully implementing the NIS2 directive. The DYNAMO project isn't endangered by it; instead, it becomes a valuable selling point for participating organizations, making framework implementation easier for them. In terms of risks, though, we can mention the unclear formulations of the directive as

such, which can lead to confusion and potential accidental non-compliance, hence it is important to ensure proper understanding of the whole directive.

The following were identified as key guidelines for implementing the NIS2 and GDPR directives in terms of the DYNAMO project:

- Legal Compliance: Hospitals must ensure that any threat intelligence sharing activities comply with both GDPR and NIS2, navigating the requirements of data protection and critical infrastructure security.
- Anonymization and Pseudonymization: Hospitals should consider anonymizing or pseudonymizing data when sharing threat intelligence to reduce the risk of unauthorized identification of individuals.
- Information Sharing Platforms: Hospitals may explore using secure and compliant information-sharing platforms that facilitate the exchange of threat intelligence while adhering to data protection regulations.
- Incident Response Planning: Hospitals should include GDPR and NIS2 compliance in their incident response plans, ensuring a coordinated and legal approach to handling cybersecurity incidents and sharing threat intelligence.
- Legal Counsel and Privacy Impact Assessments: Hospitals may seek legal counsel to assess the impact of threat intelligence sharing on GDPR compliance. Privacy Impact Assessments can help identify and address privacy risks.
- GDPR special requirements: (1) Identifying personal data in the data sets used by the DYNAMO project. (2) Designing a data protection assessment process for the DYNAMO project and the relevant subjects and performing this process in all of them. (3) Identifying tooling usable for the project and dataset automatic anonymization, to ensure only data covered by legitimate interest is shared.
- NIS2 special requirements: (1) Summarizing the value of the DYNAMO project to NIS2 implementation for the relevant clients. (2) Ensuring correct understanding of unclearly phrased phrasing inside the directive itself. (3) Based on requirements in the directive, adding activities to the project that increase its value for potential clients.

The suggested activities mainly require that a thorough review of data and policies is done. Therefore, it is also recommended to involve a lawyer in this process, as many texts to be revised need a legal opinion and approval to ensure their correctness.

6 Conclusion and Recommendations

This paper outlines the connections of the DYNAMO platform and tools to the GDPR and NIS2 directions. It's found that while the DYNAMO project needs to consider these factors, they won't be significant obstacles to its implementation. On the contrary, the DYNAMO project increases the likelihood of successful implementation of the NIS2 directive. In the case of the GDPR, while it poses some challenges, it also increases the data security of the subjects when successfully implemented.

DYNAMO's goal is to combine cyber threat intelligence and business continuity management to generate a common operational picture and shared situational awareness for decision support. Implementing NIS2 requires in many ways just that exact scope. The idea is to be prepared collectively for cyber threats in the EU. This means that everyone has situational awareness, and to be able to achieve that, different entities must be able to communicate about the identified threats before wider spread. To achieve the necessary level of response in a healthcare organization, CTI sharing between other entities is needed.

Healthcare organizations already are subject to strict privacy regulations. NIS2 adds more robust measures to protect data, respond to incidents, and mitigate cyberattacks. Although the NIS2 Directive forms the basis of the incident reporting system for providing and sharing CTI, it is up to the notifier to determine the relevant and regulation-compliant content of the notification. Determining this can be demanding for the notifying entity and can result from notifications being made as a precaution due to time limits and sanctions set by the NIS2 Directive.

This study finds that GDPR imposes some legal requirements on the DYNAMO platform, and that, on the other hand, the introduction of the NIS2 Directive provides more effective measures for CTI sharing. Further research on this topic is needed before and after the entry into force of NIS2 so that the benefits of the Directive can be truly effective.

The EU's new Artificial Intelligence Act is designed to deal with the risks of AI and aims to set clear requirements and obligations for the developers and adopters of AI. The goals of the AI Act include ensuring that AI systems comply with fundamental rights, safety, and ethical principles while addressing the risks associated with highly influential AI models. Since many DYNAMO tools

utilize AI, the requirements brought by the new Act must be carefully studied. The DYNAMO platform must be developed on this basis and legal compliance with these requirements must be demonstrated.

Acknowledgement:
This work was supported by the DYNAMO project, which has received funding from the European Union's Horizon Europe research and innovation funding program under the grant agreement no. 101069601.

References:

[1] D. Wyatt, S. Lampon and C. McKevitt, Delivering healthcare's 'triple aim': Electronic health records and the health research participant in the UK National Health Service, *Sociology of health & illness*, Vol. 42, Iss. 6, pp. 1312–1327, 2020.

[2] S. Borna, M. Maniaci, C. Haider, K. Maita, R. Torres-Guzman, F. Avila, J. Lunde, J. Coffey, B. Demaerschalk and A. Forte, Artificial Intelligence Models in Health Information Exchange: A Systematic Review of Clinical Implications, *Healthcare*, Vol. 11, Iss. 18, p. 2584, 2023, https://doi.org/10.3390/healthcare11182584.

[3] DYNAMO, Home - DYNAMO Project, 2023, [Online]. https://horizon-dynamo.eu/ (Accessed Date: January 18, 2024).

[4] ENISA, Minimum Security Measures for Operators of Essentials Services, 2022. [Online], https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services (Accessed Date: January 18, 2024).

[5] C. Laprise, It's time to take a sustainable approach to health care in the face of the challenges of the 21st century, *One Health*, Vol 16, p. 100510, 2023, https://doi.org/10.1016/j.onehlt.2023.100510.

[6] E. Frumento, Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution, in *Andreoni G, Perego P, Frumento E, (eds.) m Health Current and Future Applications*, Cham, Springer International Publishing, 2019, pp. 35-69.

[7] C. Nelson, E. Soisson, P. Li, N. Lester-Coll, H. Gagne, M. Deeley, C. Anker, L. Roy and H. Wallace, Impact of and Response to Cyberattacks in Radiation Oncology, *Adv Radiat Oncol*, Vol. 7, Iss. 5, p. 100897, 2022, https://doi.org/10.1016/j.adro.2022.100897.

[8] F. Smith, Malware and disease: Lessons from cyber intelligence for public health surveillance, *Health Security*, Vol.15, No 5, 2016. pp. 305-314.

[9] S. Wickramasinghe, Cyber Threat Intelligence (CTI): A Beginner's Guide, 2022, [Online]. https://www.splunk.com/en_us/blog/learn/cyber-threat-intelligence-cti.html#:~:text=Cyber%20threat%20intelligence%20analyzes%20threat,%2C%20tactical%2C%20and%20operati (Accessed Date: January 18, 2024).

[10] R. Sindhwani, H. Abbasi and A. Khan, Cybersecurity in healthcare: A comprehensive survey of emerging trends, challenges, and solutions, *IEEE Access*, Vol. 9, pp. 102213-102237, 2021.

[11] E. Chan, S. Foo and C. Tan, Cybersecurity challenges in healthcare: A systematic review and thematic analysis, *Journal of Medical Internet Research*, Vol. 23, Iss. 10, p. e26508, 2021.

[12] R. Sindhwani, J. Kim, H.-D. Kim and A. Khan, Cybersecurity challenges in healthcare: A focus on legacy systems and outdated software, *IEEE Access*, Vol. 8, pp. 156042-156053, 2020.

[13] Y. Wang, T. Yu, P. Zhou, W. Wang and C. Wang, Cybersecurity for medical devices: A survey, *IEEE Access*, Vol. 6, pp. 47757-47778, 2018.

[14] M. Brown, Insider threat and data security in healthcare, *Journal of Healthcare Management*, Vol. 61, Iss. 6, pp. 35-41, 2016.

[15] W. Miller, Cybersecurity challenges in healthcare: A focus on human error and phishing attacks, *JMIR mHealth and uHealth*, Vol. 9, Iss. 4, p. e17095, 2021.

[16] K. Goswami and N. Singh, Supply chain security challenges and risk mitigation strategies in healthcare industry, *Journal of Network and Computer Applications*, Vol. 156, p. 102644, 2020.

[17] S. Khan, M. Lee and S. Chae, Cybersecurity challenges in healthcare: A focus on interconnected healthcare ecosystem and its vulnerabilities, *IEEE Access*, Vol. 8, pp. 155428-155442, 2020.

[18] M. Allen and W. Smith, Regulatory compliance challenges in cybersecurity: A focus on HIPAA, *JMIR mHealth and uHealth*, Vol. 9, Iss. 3, p. e17080, 2021.

[19] E. Thompson, *Building a HIPAA-Compliant Cybersecurity Program: Using NIST 800-30 and CSF to Secure Protected Health Information*, New York: Springer Science+Business Media, 2017.

[20] M. Jalali and J. Kaiser, Cybersecurity in Hospitals: A Systematic, Organizational Perspective, *J Med Internet Res*, Vol. 20, Iss. 5, p. e10059, 2018.

[21] A. Ramsdale, S. Shiaeles and N. Kolokotronis, A comparative analysis of cyber-threat intelligence sources, formats and languages, *Electronics*, Vol 9, Iss. 5, 824, pp. 1-22, 2020, https://doi.org/10.3390/electronics9050824.

[22] P. Jayaraman, A. Forkan, A. Morshed, P. Haghighi and Y. Kang, Healthcare 4.0: A review of frontiers in digital health, *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, Vol. 10, Iss. 2, p. e1350, 2020.

[23] S. Keesara, A. Jonas and K. Schulman, Covid-19 and health care's digital revolution, *New England Journal of Medicine*, Vol. 382, Iss. 23, p. e82, 2020.

[24] M. Senbekov, T. Saliev, Z. Bukeyeva, A. Almabayeva, M. Zhanaliyeva, N. Aitenova, Y. Toishibekov and I. Fakhradiyev, The recent progress and applications of digital technologies in healthcare: a review, *International Journal of Telemedicine and Applications*, Vol. 2020, p 8830200, 2020, https://doi.org/10.1155/2020/8830200.

[25] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço and T. Cruz, ELEGANT: Security of Critical Infrastructures with Digital Twins, *IEEE Access*, Vol. 9, pp. 107574-107588, 2021.

[26] A. Al Meslamani, Why are digital health policies crucial? *Journal of Medical Economics*, Vol. 27, Iss. 1, pp. 167-169, 2024.

[27] M. Aleksandrova, Does the IP address represent personal data? [Online]. International law and tax experts - CMS international law firm. [Online], https://cms.law/en/bgr/publication/does-the-ip-address-represent-personal-data (Accessed Date: March 21, 2024).

[28] M. Horák, V. Stupka and M. Husák, GDPR compliance in cybersecurity software, *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*, August 26–29, 2019, Canterbury, United Kingdom, Artic. No. 36, pp 1-8, https://doi.org/10.1145/3339252.3340516.

[29] S. Schmitz-Berndt, Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive, *Journal of Cybersecurity*, Vol. 9, Iss. 1, p. tyad009, https://doi.org/10.1093/cybsec/tyad009.

[30] M. Negreiro, The NIS2 Directive, A high common level of cybersecurity in the EU. Briefing published by European Parliamentary Research Service, Feb. 2023, [Online]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (Accessed Date: January 20, 2024).

[31] E. Al-Qarni, Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies, *International Journal of Advanced Computer Science and Applications (IJACSA),* Vol. 14, Iss. 5, pp. 135-140, 2023.

[32] Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) 2023, [Online]. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (Accessed Date: January 20, 2024).

[33] GDPR EU. 2023. Data Protection Impact Assessment (DPIA), [Online]. https://gdpr.eu/data-protection-impact-assessment-template/ (Accessed Date: December 10, 2023).

[34] E. Rios, E. Iturbe, A. Rego, N. Ferry, J. Tigli, S. Lavirotte, G. Rocher, P. Nguyen, H. Song, R. Dautov, W. Mallouli and A. Cavalli, The DYNABIC approach to resilience of critical infrastructures, *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023),* August 29-September 01, 2023, Benevento, Italy, Artic, No. 136, pp. 1-8, https://doi.org/10.1145/3600160.3605055.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Minna Herlevi and Laura Karlsson were responsible for Section 2.
- Ville Nyman, Ilmari Pura and Jarno Virtanen were responsible for Section 3.
- Dominik Jarzemski and Jiri Kucera executed the experiments of Section 4.
- Jyri Rajamäki defined the purpose of the study, research questions and methods, supervised the work and finalized the report.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This work was supported by the DYNAMO project, which has received funding from European Union's Horizon Europe research and innovation funding programme under the grant agreement no. 101069601.

Conflict of Interest

The authors have no conflicts of interest to declare.