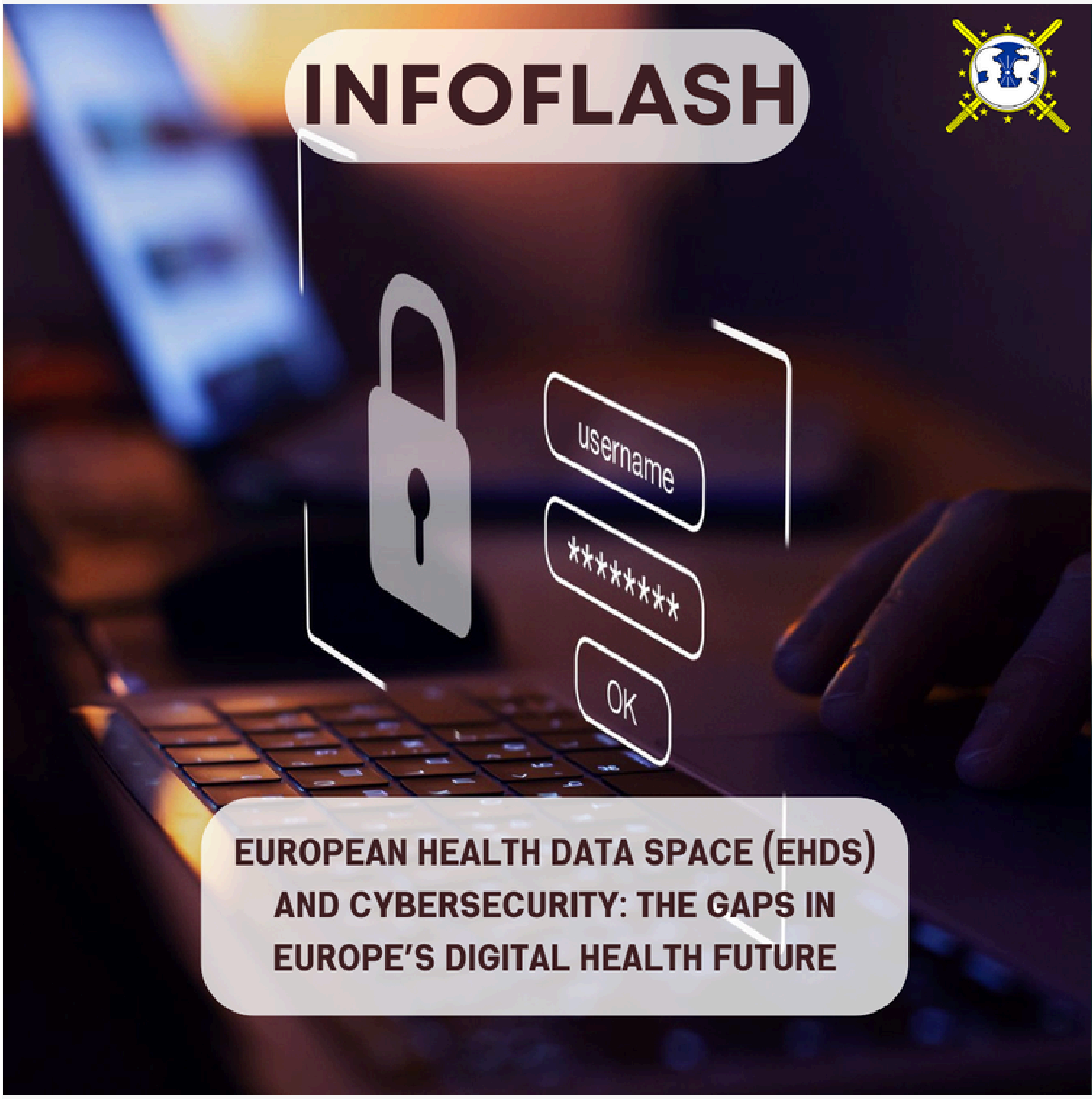
INFO FLASH
Finabel
The European Land Force
Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

FEBRUARY 2025



INFOFLASH

EUROPEAN HEALTH DATA SPACE (EHDS) AND CYBERSECURITY: THE GAPS IN EUROPE'S DIGITAL HEALTH FUTURE

WRITTEN BY
NELLIE BYLUND

EDITED BY
IVO KESLER

SUPERVISED BY
JAIME TORAL GARCÍA

Introduction

Today, the way medical data is recorded and digitised varies widely across Member States of the European Union (EU). This lack of uniformity not only makes it difficult for individuals to access their medical records across borders but also hinders the delivery of healthcare that considers a patient's complete medical history. The European Health Data Space (EHDS), expected to enter into force in 2025, aims to address these challenges by modernising and harmonising health data management within the EU. By enabling individuals to control their health data and facilitating data-sharing across the EU, the EHDS aims to improve healthcare quality and accessibility, aligning with the principles of the European Charter of Fundamental Rights, specifically the Articles of freedom of movement and integrity.

However, the EHDS also raises critical questions about privacy, cybersecurity, and the readiness of EU Member States to implement such a system. The COVID-19 pandemic underscored the need for a unified health data system, but it also revealed the vulnerabilities of digital health infrastructure to cyberattacks. The COVID-19 pandemic served as a wake-up call for the EU, highlighting the inefficiencies of fragmented health data systems. During the crisis, the EU Commission temporarily adopted the Clinical Patient Management System to allow Member States to share electronic health data. While this decision showcased the potential benefits of a unified system, it also revealed the limitations of temporary measures (European Commission, 2022). The EHDS aims to create a permanent solution, enabling seamless access to health data across borders and improving the EU's ability to respond proactively to future health crises. The EU Commission argued that "Such timely access could potentially contribute, through efficient public health surveillance and monitoring, to more effective management of future pandemics, to a reduction of costs and to improving the response to health threats, and ultimately could help to save more lives" (European Commission, 2023, p.1).

Despite the many efforts by the EU in counteracting cyber-attacks and promoting cybersecurity, incidents still occur daily. Depending on the scale of the cyber-attack, it could compromise the security of an entire nation. Consequently, failures in the EDHS system could lead to serious repercussions on a military -as well as political- level. As the EU moves forward with the EHDS, experts must discuss these cybersecurity risks to ensure that a connected health data system benefits patients without compromising their and the EU's security, safety and privacy.

1. Legal Framework

Overview of the EHDS Regulation

The EHDS Regulation builds on two fundamental EU principles: the right to freedom of movement and the right to privacy (Hasselqvist, 2023). To ensure interoperability, the Regulation requires all electronic health records (EHR) to comply with a specific exchange format. Member States must also establish digital health authorities to oversee compliance and facilitate easy access for users of their health data (European Commission, 2024).

Access to secondary health data will be governed by Health Data Access Bodies (HDABs), which will review applications, grant data permits, and ensure compliance with EHDS regulations. Each Member State appoints an HDAB, which is key in reviewing applications, granting data permits, facilitating access to electronic health records, and ensuring compliance with EHDS regulations (Ruediger & Clark, 2024). This system aims to balance the need for data sharing with protecting individual privacy.

The EHDS will operate on two levels: primary data, which allows patients and healthcare providers to access medical records anywhere in the EU, and secondary data, which supports research and public health monitoring (Brandt & Haselhofer, 2024). For patients, this means greater efficiency in receiving care abroad, as healthcare providers can instantly access their medical history, avoiding redundant tests and questions. For researchers, it means better tools for tracking health trends and predicting future threats (Brandt & Haselhofer, 2024).

Data Protection and GDPR Alignment under EHDS

The EHDS Regulation emphasises the sensitivity of health data and stresses the importance of compliance with the General Data Protection Regulation (GDPR). Therefore, health data holders are considered controllers of personal data, according to the definition provided in Article 4 No.1 of the GDPR. The system must, furthermore, adhere to the fundamental principles that work to ensure that data is Findable, Accessible, Interoperable, and Reusable, also known as the FAIR principles (European Commission, 2024). These guidelines promote transparency while respecting the GDPR's data minimisation principle. This standard is set out in Article 5.1(c) of the GDPR, which states that "Personal data shall be: [...] (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)".

Moreover, the EDHS stipulates that the rules under GDPR regarding the use of personal health data cover all types of such data, regardless of how they were collected, who provided them, or whether a public or private organization handles them. Additionally, while this Regulation grants extended rights to access and transfer personal electronic health data, these do not override or limit the existing access and portability rights already established under GDPR.

Regarding the use of secondary data in the pursuit of improved medical research, Article 9.2 of the GDPR allows for the processing of health data only under very regulated conditions, while secondary use must comply with Article 6.1 relating to the lawfulness of processing. If this provision is not complied with and health data is used outside of its intended purpose, it could result in fines up to twenty million euros, alternatively four per cent of global turnover.

One key difference between the EHDS and GDPR is the emphasis on instantaneous access to health data. While the GDPR allows up to one month for data controllers to respond to access requests, the EHDS aims to provide immediate access to health information (European Commission, 2024). This is a so-called 'complementary right' under this specific Regulation for the EHDS to function as an immediate provider of vital health information for the user.

Nonetheless, the EU Commission also considers instances where such instant access would be unethical or harmful. The Regulation provides an example where the patient might have been diagnosed with a severe terminal illness (European Commission, 2024). In those cases, the EU Commission argues that the better option is to hold back the information until health professionals can speak to the patient in person (European Commission, 2024). This is to avoid patients receiving life-altering news without the proper support system. However, this occurs in cases where it 'constitutes a necessary and proportionate measure in a democratic society' (European Commission, 2024, para 9). The Regulation reiterates that this exception still needs to be in accordance with Article 23 of GDPR, which deals with situations where certain rights, only if proportionate and necessary, can be restricted. This is to ensure that the ability to withhold certain information from the patient for their own good will not be abused or work against the purpose of the EDHS, which is free access to one's medical records.

2. Military and political implications

Cybersecurity Risks

The health sector is among the most vulnerable to cyberattacks, as highlighted by the Network and Information Security Directive's (NIS) Annual Report on Directive incidents in 2023. It concluded that ransomware attacks pose a significant threat, with cybercriminals targeting sensitive health data and demanding ransoms for their return. For example, the 2017 WannaCry attack disrupted the United Kingdom's National Health Service (NHS), causing widespread chaos and highlighting the risks of inadequate cybersecurity measures

(National Audit Office, 2017). Elisabetta Biasin argues: “A successful cyber-attack on a medical device could have severe consequences, such as compromising patient privacy and eroding trust in the healthcare system, not to mention directly harming patients' health. In the European Union (EU), where the rights to health and data protection are fundamental principles, the cybersecurity of medical devices has become a critical concern for lawmakers, policymakers, healthcare providers and medical device manufacturers” (Biasin, 2023, p. 43).

The EHDS, as a centralized system, could become a prime target for cyberattacks. If attackers gain access to the system, they could exploit personal health data for malicious purposes, such as identity theft, blackmail, or espionage. The potential for large-scale data breaches raises serious concerns about the security of the EHDS and the ability of EU Member States to protect sensitive health information.

Cybersecurity Risks and Geopolitical Threats

ENISA reported in its ‘ENISA Threat Landscape: Health Sector’, covering 2021-2023, that the European health sector faced many incidents. It concluded that ransomware was one of the leading threats to the health sector. ENISA (2024) defines ransomware as “a type of attack where threat actors take control of a target’s assets and demand a ransom in exchange for the return of the asset’s availability or in exchange for publicly exposing the target’s data” (ENISA, 2024, p.7). Cyber-criminals tend to sell sensitive information like medical history, financial information, demographic details and similar data retrieved from a personal health record of an individual on the black market (Raizada & Biswal, 2024).

The health sector’s vulnerability to cyberattacks has significant military and political implications. Hacktivist groups, often linked to state-affiliated actors, have increasingly targeted critical infrastructure, including healthcare systems. For instance, during the war in Ukraine, hacktivist groups aligned with both sides carried out cyberattacks on healthcare facilities, disrupting services and exposing sensitive data (ENISA, 2024).

One prevalent issue in countering cyberattacks through legislation, such as the ones the EU has imposed, is the speed at which cyber attackers develop and adapt. Moreover, these examples showcase that even the smallest groups can present real military threats to, in extreme cases, entire states through cyber operations, meaning that the law, which has traditionally dealt with conflicts between state versus state or state versus non-state armed groups, now needs to adapt to a new type of warfare (Feichtinger, 2014). Consequently, cyber-attacks and cybersecurity are and should be, of great importance to EU Member States on both a military and political level.

The Ponemon Institute concluded in a study in 2018 that some of the cyber threats with the greatest risks were, inter alia, cyber warfare/terrorism, breaches involving high-value information and breaches that damage critical infrastructure (Bernabe & Skarmeta, 2019). It concluded that those categories will have “the greatest impact on organizations over the next three years” (Bernabe & Skarmeta, 2019, p.8). The EHDS, as a collective system, could become a target for state-sponsored cyberattacks aimed at destabilising the EU. The potential for large-scale data breaches raises questions about the EU’s ability to defend its critical infrastructure and respond to cyber threats.

In extreme cases, a successful attack on the EHDS could have far-reaching consequences, affecting individual patients and national security. This has also been highlighted in ENISA’s report ‘Foresight Cybersecurity Threats For 2030’, which states: “The rise of technology-driven criminal activities has prompted discussions about the need for alternative enforcement mechanisms. Some have proposed stronger international cooperation, updated legal frameworks, and increased investments in cybersecurity and digital forensics to combat these evolving threats effectively” (ENISA, 2024, p.19). A collective, uniform healthcare system such as EDHS presents many risks and challenges. Experts have widely discussed the perks of a collective system of medical records, but they still need to give more consideration to the cons. Keeping in mind the disparity between EU Member States in technological advancements, the question of all EU nations being able to ensure the security of personal data within EDHS needs to be raised.

Having one collective health data system might increase its vulnerability to cyber-attacks as the attacker(s) would, technically, only must find a way into one system to be able to access a wide range of natural persons’ data. Arguably, the medical data of natural persons within the EU is not of such nature as to be classified as ‘high-value data’ or present a cyber threat to a degree which would be relevant on a military level. However, with access to a person's medical records the cyber attacker could use the data accessed to, inter alia, exercise what scholars have defined as ‘Identification of Personal Weak Spots’, ‘Personalised Persuasion’ and ‘Contacting the Data Subject’ (Kröger et al., 2021). Moreover, the data could be used for espionage purposes, meaning operations conducted with the purpose of ‘gaining information on IP (intellectual property), sensitive data, classified data’ (ENISA, 2024). This situation could have serious consequences not only on the individual level but for the security of a whole nation if attacks would be on a larger scale.

If a cyber-attack on critical infrastructure, such as hospitals, would reach such levels as to affect a nation, the questions extend far beyond these considerations. They encompass a broad range of issues related to hybrid-warfare, especially under International Law, including the right to self-defence and the responsibility to protect—matters that traditionally fell within the exclusive domain of state sovereignty (Kröger et al, 2021). As a critical digital health infrastructure, the EHDS could become a target for state-sponsored cyberattacks. If so, it could trigger Article 42.7 of the Treaty on European Union, meaning the mutual defence clause. However, it is important to note that the question of when a cyber attack would reach the level as to invoke the right to self-defence is highly debated (Oorsprong, Ducheine et al., 2022).

EU Initiatives and Defence Strategies

While the risks are significant, the EHDS also has the potential to improve cybersecurity across the EU. By standardising data protection measures and requiring high levels of security, the Regulation could help raise the overall level of cybersecurity in Member States (Ruediger, Clark, 2024). Additionally, the EU has launched several initiatives to strengthen cybersecurity, including Cyber Rapid Response Teams and a Cyber Emergency Response Fund. Notably, international cooperation will also be essential, as exemplified by the FBI and Spain's cooperation in the case of a cybercriminal group known as Gold Harvest (ENISA, 2024) since cyberattacks often originate outside the EU. By working together, Member States can develop a more resilient and secure health data system.

Moreover, the EU has implemented several cybersecurity initiatives and legal frameworks. Apart from the previously discussed GDPR, the EU has a wide range of laws to ensure cybersecurity in medical devices. These include Medical Device Laws, Cybersecurity Laws, including the Network Information System Directives and the Cybersecurity Act, AI Laws and Data Laws, including the Data Act. These efforts aim to enhance the EU's overall cybersecurity and ensure a coordinated response to cyber threats. While these frameworks enhance the overall persistence of digital infrastructure, their decentralised implementation by Member States could lead to disparities in cybersecurity protections across different countries. This fragmentation poses risks, as cyber threats do not respect national borders, while inconsistencies in security measures could create weak points within the EHDS network. Despite these increased and improved cybersecurity efforts, scholars have argued that the health sector is one of the less developed sectors in terms of cybersecurity (van Kessel et al., 2023). Additionally, as noted by van Kessel in an article in the Journal of Medical Internet Research, "Disruptive attacks and lack of network segmentation allow foreign bodies to access the entire network instead of subsections, as well as exfiltrate sensitive information about the digital environment, which had a significant impact on the health sector". Considering that this is a prevalent issue, the question is whether a collective system will counteract these security issues or make them even more widespread.

Despite the EU's many cybersecurity initiatives which lay the groundwork for protecting digital infrastructure, breaches of protected data still occur every day. Therefore, their future effectiveness in securing the EHDS will depend on the extent to which Member States align their policies and collaborate to address emerging cyber threats.

Conclusion

The European Health Data Space represents a transformative step towards modernising healthcare data management across the EU, promising improved accessibility, interoperability, and patient control over personal health data. However, as this article has highlighted, the initiative also introduces significant cybersecurity challenges that must be addressed to ensure its success. The health sector's vulnerability to cyberattacks, coupled with the political and military implications of large-scale data breaches, underscores the need for robust legal, technical, and collaborative measures.

To mitigate these risks, the EU must prioritise a unified approach to cybersecurity, pushing existing frameworks like GDPR while investing in advanced technologies and international cooperation. The EHDS has the potential to serve as a fundamental improvement in healthcare delivery and set a global standard for secure health data sharing. However, its success will depend on the EU's ability to balance innovation with security, ensuring that the benefits of an interconnected health data system do not come at the expense of patient privacy and safety. As the EHDS approaches its implementation, ongoing dialogue among policymakers, cybersecurity experts, and healthcare providers will be essential to navigate the complex challenges ahead and build a trustworthy system for all EU citizens.

If regulated properly, the implementation of EDHS could be revolutionary for interoperability across EU Member States and medical health care as a whole. As this is a new regulation that has not yet completely entered into force, follow-ups and adjustments regarding the cybersecurity of EDHS will surely follow. If regulated properly, the implementation of EDHS could be revolutionary for interoperability across EU Member States and medical health care as a whole. However, many questions remain unanswered. Loopholes for cyber-attackers can always be found, and technology advances faster than any law could. This leaves the issue of effective cyber-attack countermeasures continuously relevant and the future of private data uncertain.

Bibliography

Biasin, E., Yasar, B., & Kamenjasevic, E. (2023, November 21). New cybersecurity requirements for medical devices in the EU: The forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act. Law, Technology and Humans, 5(2), 43–58.
https://lthj.qut.edu.au/article/view/3068?utm

Brandt, V., & Haselhofer, K. (2024). Revolution inom hälsodata: En förändring av tillgången till och användare av hälsodata inom hälso- och sjukvård, forskning samt innovation - del 1. Knowit.
https://blogg.knowit.se/revolution-inom-h%C3%A4lsodata-en-f%C3%B6r%C3%A4ndring-av-tillg%C3%A5ngen-till-och-anv%C3%A4ndande-av-h%C3%A4lsodata-inom-h%C3%A4lso-och-sjukv%C3%A5rd-forskning-samt-innovation-del-1

European Commission. (2025, January 15). Cybersecurity of hospitals and healthcare providers. European Commission.
https://digital-strategy.ec.europa.eu/en/library/cybersecurity-hospitals-and-healthcare-providers

European Health Data Space. (2022, May 3). Regulation 2022/0140 of the European Parliament and of the Council on the European Health Data Space. Official Journal of the European Union.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197

European Health Data Space. (2024, November 20). Regulation 2024/2847 of the European Parliament and of the Council on the European Health Data Space. Official Journal of the European Union.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847

European Union Agency for Cybersecurity. (2024, April 30). Foresight cybersecurity threats for 2030 - Update 2024: Extended report.
https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report

European Union Agency for Cybersecurity. (2024, September 19). Threat landscape. European Union Agency for Cybersecurity.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Feichtinger, W. (2014). Editorial: Hybride Kriegführung und Cybersicherheit / Editorial: Hybrid warfare and cyber security. Sicherheit Und Frieden (S+F) / Security and Peace, 32(1), III–IV. https://www.jstor.org/stable/i24218472?utm

Hasselqvist, P. (2023, April 20). Det europeiska hälsodataområdet (EHDS). Sveriges Kommuner och Regioner (SKR). https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/euforordningareudirektivdigitalisering/forslag/deteuropeiskahalsodataomradetehds.70268.html?utm

Megatrends. (2018, March 15). Study on global mega trends since cybersecurity. Ponemon Institute research report. https://www.ponemon.org/news-updates/blog/security/ponemon-institute-announces-the-release-of-the-2018-megatrends-study.html

Morse, A. (2017, October 27). Investigation: WannaCry cyber attack and the NHS. National Audit Office. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/?utm

Network and Information Security Directive's (NIS). (2024, October). Annual report NIS Directive incidents 2023. CG Publication. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group?utm

Oorsprong, F., Ducheine, P., & Pijpers, P. (2023, February 22). Cyber-attacks and the right of self-defense: A case study of the Netherlands. Policy Design and Practice, 6(2), 217–239. https://www.tandfonline.com/doi/full/10.1080/25741292.2023.2179955

Raizada, N., & Biswal, M. (2024, May). An evidence-based investigation of CERT-IN's reporting on cyber-threats in the healthcare sector. Conhecimento & Diversidade, Niterói, 16(42). https://www.researchgate.net/publication/381540234_AN_EVIDENCE-BASED_INVESTIGATION_OF_CERT-IN'S_REPORTING_ON_CYBER-THREATS_IN_HEALTHCARE_SECTOR

Rudiger, A., & Clark, J. (2024, November 19). EHDS – Access to health data for secondary use under the European Health Data Space. DLA Piper. https://privacymatters.dlapiper.com/2024/11/eu-ehds-access-to-health-data-for-secondary-use-under-the-european-health-data-space/

Terzis, P. (2022, October 27). Compromises and Asymmetries in the European Health Data Space. European Journal of Health Law, 30(3), 345-363.
https://brill.com/view/journals/ejhl/30/3/article-p345_5.xml

Van Kessel, R., Haig, M., & Mossialos, E. (2023, August 24). Strengthening cybersecurity for patient data protection in Europe. Journal of Medical Internet Research, 2.
https://www.jmir.org/2023/1/e48824/citations