Viewpoint

Strengthening Cybersecurity for Patient Data Protection in Europe

Robin van Kessel[1], PhD; Madeleine Haig[1], MSc; Elias Mossialos[1,2], PhD

[1]LSE Health, Department of Health Policy, London School of Economics and Political Science, London, United Kingdom

[2]Institute of Global Health Innovation, Imperial College London, London, United Kingdom

Corresponding Author:
Elias Mossialos, PhD
LSE Health
Department of Health Policy
London School of Economics and Political Science
Houghton Street
London, WC2A 2AE
United Kingdom
Phone: 44 7772 707841
Email: e.a.mossialos@lse.ac.uk

Abstract

The health care sector experiences 76% of cybersecurity breaches due to basic web application attacks, miscellaneous errors, and system intrusions, resulting in compromised health data or disrupted health services. The European Commission proposed the European Health Data Space (EHDS) in 2022 to enhance care delivery and improve patients' lives by offering all European Union (EU) citizens control over their personal health data in a private and secure environment. The EU has taken an important step in homogenizing the health data environment of the European health ecosystem, although more attention needs to be paid to keeping the health data of EU citizens safe and secure within the EHDS. The pooling of health data across countries can have tremendous benefits, but it may also become a target for cybercriminals or state-sponsored hackers. State-of-the-art security measures are essential, and the current EHDS proposal lacks sufficient measures to warrant a cybersecure and resilient environment.

(J Med Internet Res 2023;25:e48824) doi: 10.2196/48824

KEYWORDS

cybersecurity; Europe; European Health Data Space; digital health; mHealth; medical informatics; data privacy; patient safety; privacy; health service

Globally, 1463 cyberattacks were reported per week in 2022, with an average cost per breach of approximately US $10 million [1]. The European Union Agency for Cybersecurity (ENISA) reported that the health care sector in the European Union (EU) experienced 76% of cybersecurity breaches due to basic web application attacks, miscellaneous errors, and system intrusions in 2021. Internal threat actors also remained prominent, accounting for 39% of cybersecurity breaches [2]. The health care sector also faced numerous high-impact cybersecurity incidents that compromised sensitive data or disrupted health services, currently amounting to a median cost of €300,000 (US $325,000) per major security incident [3]. Additionally, the health care sector is one of the less mature sectors in the field of cybersecurity [4]. 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. The societal migration to the digital world because of the COVID-19 pandemic worsened this situation, as fear and uncertainty among the public rose, resulting in a higher susceptibility to being exposed to harmful digital content and cybersecurity threats [5-8]. In fact, a 5-fold increase in cybercrimes was observed by the World Health Organization during the first 2 months of the pandemic [9]. This was further compounded by the distribution of counterfeit COVID-19 products on the dark web [10].

The European Commission proposed the European Health Data Space (EHDS) in 2022 to enhance care delivery and improve patients' lives by offering all EU citizens control over their personal health data in a private and secure environment. The goal was to eliminate information barriers and establish a single market for digital health services [11]. More specifically, the EHDS enabled EU citizens to provide health professionals throughout the EU with access to their personal health data via a digital interface. This system would streamline the use of health data for purposes like research, innovation, policy making, and regulatory tasks, all the while upholding complete adherence to the EU's data protection standards [11]. Rooted in the fundamental principles of civic participation and empowerment that define the EU, the EHDS also addresses obstacles hindering the broad acceptance of digital health methods in conventional health care [12,13]. Although concerns have been raised about the current iteration of the EHDS proposal, including its potential to exacerbate health inequalities instead of remedying them [14] and potential changes to data-sharing practices [15], the concept of cybersecurity has received limited attention.

The EHDS proposal only briefly mentions cybersecurity as a field that should be coordinated and collaborated with throughout the proposal (articles 10 [2], 39 [1], and 64 [5]) [5]. However, a global shortage of cybersecurity professionals in all domains was reported in a recent review on improving cybersecurity education [16]. One example of this is the recent release of the Cybersecurity Skills Academy by the European Commission, which was created to help close the cybersecurity talent gap and boost the EU's competitiveness, growth, and resilience in cybersecurity [17]. Still, relying on a single supply source for cybersecurity professionals may be challenging due to significant labour market demand. One possible solution is to explore the feasibility of incorporating cybersecurity modules into medical, public health, and digital health curricula and providing retraining and upskilling opportunities for practicing professionals [16]. However, to achieve this, cybersecurity must be recognized and added as a core competency of digital health professionals, similar to what NHS Health Education England has implemented [18,19].

The EHDS proposal refers to the updated Network and Information Security Directive as a common cybersecurity framework [20], which requires EU member states to adopt various measures to improve their national cybersecurity environments. However, as a Directive, it leaves the responsibility to the member states to determine the means by which the objectives outlined in the Directive are achieved. This could pose a significant cybersecurity threat to the EU due to the divergent national cybersecurity strategies and resources allocated to achieve them [21]. EU member states with limited digital and cybersecurity capabilities, such as Southern or Eastern member states or small states, may be particularly vulnerable to coordinated attacks aimed at denying service and gaining unauthorized access [4,22]. To begin rectifying these disparities in digital infrastructure within the EU, one potential approach could involve the European Commission leveraging its extensive track record of infrastructure investments. This could entail establishing a dedicated investment portfolio aimed at extending digital infrastructure into underserved nations and communities.

A uniform cybersecurity system across the EU, and in particular, in the context of the EHDS, could provide a more comprehensive security net and enable the introduction of an EU-wide cybersecurity training curriculum. This system can include segmentation, multifactor authentication, and the use of virtual local area networks and cloud computing as well as training employees, monitoring behaviour, reducing human error, and enhancing stakeholder alignment [23,24]. Regarding segmentation, it is important to highlight that even though the system might be segmented on a national, regional, or local scale, all these segments would still operate within a unified federated network. In essence, despite being divided into numerous segmented networks, the system retains the ability to function as a cohesive, comprehensive network. In cases of cybersecurity threats, it is also feasible to isolate certain parts of the system to prevent the threat from infiltrating the federated network. Notably, recent technological advancements have demonstrated promising progress in the realm of cybersecurity. Technologies like blockchain [25-27] and a community solid server, which furnishes individuals with their personal data storage spaces [28], have been effective in addressing concerns related to patient privacy breaches. Furthermore, technologies such as Fast Healthcare Interoperability Resources (which dictate rules for exchanging electronic health care data) [29-31], the Observational Medical Outcomes Partnership Common Data Models (a standardized data format to facilitate consistent analysis of observational data) [32], and cross-enterprise document sharing (enabling cataloguing and sharing of patient records across health care institutions) are also capable of addressing cybersecurity issues tied to electronic health records [33]. Nevertheless, implementing effective cybersecurity measures may come at an additional cost; however, these costs are relatively insignificant compared to the direct costs of cybersecurity threats (mentioned above) and the potential direct and indirect repercussions of exposing the health data of EU citizens to substandard cybersecurity practices [2].

ENISA was created in 2019 to develop a high uniform level of cybersecurity within the EU and standardize and improve cybersecurity across its member states. However, its mandate is currently limited to providing technical and human resources to support EU member states, conducting reviews of cybersecurity policies and threats in the EU, and facilitating the exchange of best practices among the member states [22]. Although ENISA was established to enhance EU cybersecurity, the scope of its mandate prevents it from taking a leading role in the development of cybersecurity policies and resources. To achieve a homogeneous cybersecurity environment, ENISA's mandate needs to be expanded to proactively build and coordinate cybersecurity policies within EU member states and create a set of common cybersecurity standards. This would require the European Commission and EU member states to acknowledge the importance of addressing cybersecurity at the EU level [34]. By doing so, the EU can reduce potential negative consequences of divergent cybersecurity policies and build a stronger cybersecurity workforce to ensure the security of sensitive data within the EHDS and the health care sector. Additionally, this approach would enable ENISA to use its expertise and data related to cybersecurity threats. This could involve creating precise benchmarks for evaluating the affordability and sustainability of the EU cybersecurity system and assessing its cost-effectiveness—an area that currently lacks established criteria. Moreover, this strategy would empower ENISA to draw upon its industry-specific insights, enabling it to propose exemplary practices that harmonize with the digital capacities and preparedness of distinct industries.

The EU has taken a significant step toward homogenizing the health data environment in the European health ecosystem, but more attention is needed to ensure the safety and security of the health data of EU citizens within the EHDS. Although pooling health data across countries can bring tremendous public health benefits, it can also become a prime target for cybercriminals or state-sponsored hackers, posing a significant risk to EU citizens. Therefore, state-of-the-art security measures are essential, and the current iteration of the EHDS proposal does not contain sufficient measures to create a cybersecure and resilient environment.

Conflicts of Interest

None declared.

References

1. Cost of a Data Breach Report 2023: fight back against data breaches. IBM. URL: https://www.ibm.com/reports/data-breach [accessed 2023-08-22]
2. ENISA threat landscape 2022: July 2021 to July 2022. EU Publications. URL: https://op.europa.eu/en/publication-detail/-/publication/791dcc19-922e-11ed-b508-01aa75ed71a1/language-en [accessed 2023-08-22]
3. NIS investments: November 2022. EU PUblications. URL: https://data.europa.eu/doi/10.2824/433214 [accessed 2023-08-22]
4. Tasheva I, Kunkel I. In a hyperconnected world, is the EU cybersecurity framework connected? European View 2022 Nov 20;21(2):186-195 [doi: 10.1177/17816858221136106]
5. Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity risks in a pandemic. J Med Internet Res 2020 Sep 17;22(9):e23692 [FREE Full text] [doi: 10.2196/23692] [Medline: 32897869]
6. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: a survey. J King Saud Univ Comput Inf Sci 2022 Nov;34(10):8176-8206 [FREE Full text] [doi: 10.1016/j.jksuci.2022.08.003] [Medline: 37521180]
7. Holly L, Wong BLH, van Kessel R, Awah I, Agrawal A, Ndili N. Optimising adolescent wellbeing in a digital age. BMJ 2023 Mar 20;380:e068279 [FREE Full text] [doi: 10.1136/bmj-2021-068279] [Medline: 36940933]
8. Roman-Urrestarazu A, Kinsey J, van Kessel R. A bill of children's digital rights is required to improve and sustain children's futures globally. JAMA Pediatr 2022 Nov 01;176(11):1064-1066 [doi: 10.1001/jamapediatrics.2022.3418] [Medline: 36155616]
9. WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. 2020 Apr 3. URL: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance [accessed 2023-08-06]
10. Catalani V, Townshend HD, Prilutskaya M, Roman-Urrestarazu A, van Kessel R, Chilcott RP, et al. Profiling the vendors of COVID-19 related product on the Darknet: an observational study. Emerg Trends Drugs Addict Health 2023;3:100051 [FREE Full text] [doi: 10.1016/j.etdah.2023.100051] [Medline: 37020522]
11. European Health Union: A European Health Data Space for people and science Internet. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711 [accessed 2022-05-04]
12. Wong BLH, Maaß L, Vodden A, van Kessel R, Sorbello S, Buttigieg S, European Public Health Association (EUPHA) Digital Health Section. The dawn of digital public health in Europe: implications for public health policy and practice. Lancet Reg Health Eur 2022 Mar;14:100316 [FREE Full text] [doi: 10.1016/j.lanepe.2022.100316] [Medline: 35132399]
13. Marelli L, Stevens M, Sharon T, Van Hoyweghen I, Boeckhout M, Colussi I, et al. The European health data space: too big to succeed? Health Policy 2023 Sep;135:104861 [doi: 10.1016/j.healthpol.2023.104861]
14. van Kessel R, Wong BLH, Forman R, Gabrani J, Mossialos E. The European Health Data Space fails to bridge digital divides. BMJ 2022 Jul 08;378:e071913 [doi: 10.1136/bmj-2022-071913] [Medline: 35803600]
15. Shabani M. Will the European Health Data Space change data sharing rules? Science 2022 Mar 25;375(6587):1357-1359 [doi: 10.1126/science.abn4874] [Medline: 35324305]
16. AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Raymond Choo K. The role of national cybersecurity strategies on the improvement of cybersecurity education. Comput Secur 2022 Aug;119:102754 [doi: 10.1016/j.cose.2022.102754]
17. Cyber Skills Academy. Digital Skills & Jobs Platform. 2023. URL: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy [accessed 2023-05-08]
18. Artificial intelligence (AI) and digital healthcare technologies capability framework. NHS Health Education England: Digital Transformations. URL: https://digital-transformation.hee.nhs.uk/building-a-digital-workforce/dart-ed/horizon-scanning/ai-and-digital-healthcare-technologies [accessed 2023-05-08]
19. van Kessel R, Roman-Urrestarazu A, Anderson M, Kyriopoulos I, Field S, Monti G, et al. Mapping factors that affect the uptake of digital therapeutics within health systems: scoping review. J Med Internet Res 2023 Jul 25;25:e48000 [FREE Full text] [doi: 10.2196/48000] [Medline: 37490322]
20. NIS2 Directive. European Commission. URL: https://eur-lex.europa.eu/eli/dir/2022/2555 [accessed 2023-04-10]
21. Markopoulou D, Papakonstantinou V, de Hert P. The new EU cybersecurity framework: the NIS Directive, ENISA's role and the General Data Protection Regulation. CLSR 2019 Nov;35(6):105336 [doi: 10.1016/j.clsr.2019.06.007]
22. Martti L. Cyber-attacks against critical infrastructure. In: Cyber Security. Cham, Switzerland: Springer International Publishing; 2022:3-42

23. Stern AD, Gordon WJ, Landman AB, Kramer DB. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. BMJ Open 2019 Jun 28;9(6):e025374 [FREE Full text] [doi: 10.1136/bmjopen-2018-025374] [Medline: 31256020]
24. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. THC 2017 Feb 21;25(1):1-10 [doi: 10.3233/thc-161263]
25. Roehrs A, da Costa CA, da Rosa Righi R. OmniPHR: a distributed architecture model to integrate personal health records. J Biomed Inform 2017 Jul;71:70-81 [FREE Full text] [doi: 10.1016/j.jbi.2017.05.012] [Medline: 28545835]
26. Madine MM, Salah K, Jayaraman R, Yaqoob I, Al-Hammadi Y, Ellahham S, et al. Fully decentralized multi-party consent management for secure sharing of patient health records. IEEE Access 2020;8:225777-225791 [doi: 10.1109/access.2020.3045048]
27. Misbhauddin M, AlAbdulatheam A, Aloufi M, Al-Hajji H, AlGhuwainem A. MedAccess: a scalable architecture for blockchain-based health record management. 2020 Presented at: 2nd International Conference on Computer and Information Sciences (ICCIS); Oct 13-15; Sakaka, Saudi Arabia p. A [doi: 10.1109/ICCIS49240.2020.9257720]
28. Celuchova Bosanska D, Huptych M, Lhotská L. Decentralized EHRs in the semantic web for better health data management. Stud Health Technol Inform 2022 Nov 03;299:157-162 [doi: 10.3233/SHTI220975] [Medline: 36325857]
29. Spratt S, Ravneberg D, Derstine B, Granger B. Feasibility of electronic health record integration of a SMART application to facilitate patient-provider communication for medication management. Comput Inform Nurs 2022 Aug 01;40(8):538-546 [doi: 10.1097/CIN.0000000000000891] [Medline: 35234708]
30. Lobach DF, Boxwala A, Kashyap N, Heaney-Huls K, Chiao AB, Rafter T, et al. Integrating a patient engagement app into an electronic health record-enabled workflow using interoperability standards. Appl Clin Inform 2022 Oct 14;13(5):1163-1171 [FREE Full text] [doi: 10.1055/s-0042-1758736] [Medline: 36516969]
31. Bender D, Sartipi K. HL7 FHIR: an agile and RESTful approach to healthcare information exchange. 2013 Presented at: 26th IEEE International Symposium on Computer-Based Medical Systems; June 20 - 22; Porto, Portugal [doi: 10.1109/cbms.2013.6627810]
32. Standardized data: the OMOP common data model. OHDSI. URL: https://www.ohdsi.org/data-standardization/ [accessed 2023-07-24]
33. Noumeir R, Renaud B. IHE cross-enterprise document sharing for imaging: interoperability testing software. Source Code Biol Med 2010 Sep 21;5(1):9 [FREE Full text] [doi: 10.1186/1751-0473-5-9] [Medline: 20858241]
34. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) Internet. European Commission. 2019 Apr. URL: http://data.europa.eu/eli/reg/2019/881/oj/eng [accessed 2023-04-17]

Abbreviations

EHDS: European Health Data Space
ENISA: European Union Agency for Cybersecurity
EU: European Union

Edited by A Mavragani; submitted 08.05.23; peer-reviewed by M Gong, R Marshall; comments to author 18.07.23; revised version received 07.08.23; accepted 16.08.23; published 24.08.23

Please cite as:
van Kessel R, Haig M, Mossialos E
Strengthening Cybersecurity for Patient Data Protection in Europe
J Med Internet Res 2023;25:e48824
URL: https://www.jmir.org/2023/1/e48824
doi: 10.2196/48824
PMID: