This policy was adopted by the 7th EMSA Spring Assembly held online on the 10th of April of 2021. Must be reconsidered until: 10th of April of 2025.

Cybersecurity in Healthcare

Authors: Stella Goeschl, Natasha Lalenya Barbour-Murray, Büşra Buzkartaca, Taylan Deniz Kuzu, Iulia-Alexandra-Simona Bretea, Şoreş Dinar

The European Medical Students´ Association (EMSA) represents medical students across Europe. We envision a healthy and solidary Europe in which medical students actively promote health. EMSA empowers medical students to advocate health in all policies, excellence in medical research, interprofessional healthcare education and the protection of human rights across Europe.

Executive Summary

Cybersecurity is increasingly relevant in the healthcare sector due to the growing use of digital health solutions. The pursuit of precision care through digital technologies in medical practise has put healthcare institution networks at substantial risk of cyber threats and data leaks. As the healthcare system stores sensitive patient data and deals with highly vulnerable populations in this context, the protection of patient data is crucial. Necessary measures must be taken regarding policy making in the healthcare sector on a national and regional level to ensure the highest standard of cybersecurity. EMSA recognizes the importance of proper cybersecurity for healthcare systems and advocates on behalf of future healthcare professionals in a digital healthcare field.

Problem Statement

Health data falls under the category of sensitive data as defined by the European Commission. It thus warrants special protection and falls under specific regulations under EU law. The processing of sensitive data must be done with adequate security measures in place (European Commission, 2019).

With the rise of the COVID-19 crisis, the use of digital technologies has seen a marked increase. In the wake of the pandemic, healthcare is broadly entering the digital age. Whilst there is no doubt that digital innovations can be beneficial to healthcare administrations and patient outcomes, there are a number of drawbacks. The main concern for the healthcare industry in the coming years is, and will be, cybersecurity.

There are a number of ways in which threats can be established in healthcare. These include data theft, hacking of medical devices, and the deletion or corruption of data which may not be detected for many years. All of these methods can cause indirect and direct harm to patients.

A pertinent example of healthcare systems being the focus of a malicious attack would be the 2017 WannaCry Ransomware attack that struck the UK's National Health Service. This attack resulted in the loss of access to healthcare systems, meaning treatment plans had to be delayed, operations cancelled and incoming ambulances rerouted (Argaw, 2020). In addition to this, there were financial consequences of long term effects on treatments and additional medication provided for patients.

Vulnerabilities are not isolated to systems, servers, and websites. As devices such as pacemakers are connected to the internet, classifying them as IoT (Internet of Things) devices, it isn't just data that becomes compromised; the operationality of medical devices and patient safety are also jeopardised. An important aspect of medicine is the trust that lies between a patient and their doctor. The breach of this trust in any manner is detrimental (Argaw, 2020).

Our View. Aim.

In recent years, medical innovations have focused on creating and implementing digitally reliant medical devices and software. These aim to improve the delivery of healthcare services, resulting in increased precision.

The creation of technology that is meant to handle both personally identifiable and protected health information, both of which imply invaluable damage if lost, requires prolonged experimentation and implementation time. However, implementation of proper cybersecurity technology can present a considerable cost factor for healthcare providers, among other implementation barriers.

Currently, many healthcare providers use outdated software, often handled by insufficiently instructed medical staff. In addition to this, the intrinsic nature of online databases makes them vulnerable to system breaches. There is an increasing awareness and demand to counteract these vulnerabilities. However, though resources are spent on design and implementation of technology and necessary means, there is still a lack in the adoption of adequate cyber protection measures that could minimise damage and secure patient security and thus maintain patient trust.

All aspects of patient safety, data protection, and privacy, are of the highest priority and must be handled as such. Thus, it is crucial that healthcare security is prioritised going forward. The nature of the unique information relevant to healthcare systems means that the risk and consequences are infinitely more significant than those in other sectors, particularly considering the vast quantity of personal and sensitive information held in health records. As technologies grow in complexity and breadth of use and innovation, emerging vulnerabilities and the need for adaptable security measures have become increasingly evident (Ghafur, 2019).

Recommendations

EMSA calls upon the European Institutions to:

- Include education and training on cybersecurity of health professionals in their agenda;
- Support strategies for investment and implementation of protections to IoT, stationary and mobile devices, including encryption;
- Support an interprofessional network to boost the exchange of professions and stakeholders regarding cybersecurity in healthcare;
- Collaborate with the European Union Agency for Cybersecurity (ENISA) to provide a comprehensive cybersecurity infrastructure in the European realm.
- Lead and promote an international communication campaign to sensitise people to the benefits of digital health solutions.

EMSA calls upon European medical faculties to:

- Ensure education and training on cybersecurity in the medical curriculum, not exclusive to but including encryption and ethical matters;
- Create a culture of constructive criticism and error tolerance that re-enforces security and the required actions needed.

EMSA calls upon IT-collectives to:

- Participate in the public dispute on the topic of cybersecurity in healthcare settings;
- Raise awareness on deficits within the framework of cybersecurity

EMSA calls upon European Member States to:

- Invest and implement protections to IoT, stationary and mobile devices, including encryption;
- Provide safe storage and access to sensitive data:
    - Invest in and implement a separate backup-framework of sensitive data;
    - Ensure adequate end-to-end encryption to limit access to sensitive data;
- Include education and training of health professionals on cybersecurity in the agenda:
    - Support national projects/initiatives and boost the exchange of best practices for the implementation of education and training on cybersecurity into medical education;
- Analyse, evaluate and re-evaluate the status of implementation of proper cybersecurity mechanism in their respective health systems;
- Collaborate with ENISA to provide a comprehensive cybersecurity infrastructure in the European realm;
- Adhere to the NIS directive and transpose mentioned measures on a national level.

EMSA calls on European Medical Student Organizations and commits itself to:

- Acknowledge the relevance of education and training on cybersecurity for present and future health professionals;
- Implement education and training on cybersecurity as a part of the European core curriculum with periodic updates;
- Raise awareness among their members regarding the significance of cybersecurity, its threats and its promises.

Conclusion

Healthcare data is considered sensitive data and requires special protection. When compared to other industries, the healthcare industry lacks security measures to defend its network, machines and data. It is paramount to take necessary precautions to shield healthcare systems from cyber attacks.

EMSA calls on European Institutions and European Member States to implement and develop strategies to create safe and updated networks, train health professionals on cybersecurity and finally supervise and constantly update the protection systems to ensure the safety of network data. EMSA calls on medical students organisations and commits itself to acknowledge the threats to cybersecurity and raise awareness on a large scale.

Definitions

ENISA: European Union Agency for Cybersecurity

Cybersecurity: "Cybersecurity comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats." (ENISA, 2020)

Cybercrime: "refers to any crime/criminal activity facilitated by or using cyber space" (ENISA, 2020)

Internet of Things (IoT): "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making" (ENISA, 2020)

References

- Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1). https://doi.org/10.1186/s12911-020-01161-7

- Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113(113), 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

- Sensitive data. (n.d.). Commission.europa.eu. Retrieved March 21, 2023, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data_en

- ENISA. (n.d.). Www.enisa.europa.eu. https://www.enisa.europa.eu

- Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health, 1(1), e10–e12. https://doi.org/10.1016/s2589-7500(19)30005-6

- Cs, K., B, F., T, J., & Dk, M. (2017). Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. Technology and Health Care : Official Journal of the European Society for Engineering and Medicine. https://pubmed.ncbi.nlm.nih.gov/27689562/

- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? BMJ, 358, j3179. https://doi.org/10.1136/bmj.j3179