HealthManagement
Promoting Management and Leadership

ENISA Procurement Recommendations on Cybersecurity

The European Union Agency for Cybersecurity (ENISA) has released cybersecurity guidelines for hospitals when procuring services, products and infrastructure, identifying relevant threats and risks and mapping good practices.

You might also like: ENISA director, Juhan Lepassaar, explains how the COVID-19 pandemic has made the need for effective cyber hygiene even more urgent. Read more

Digitalisation of healthcare has seen an explosive growth during the COVID-19 pandemic, especially in terms of virtual health and telemedicine. At the same time, cyber threats and data protection-related issues have come to the forefront. ENISA's new report, *Cloud Security for Healthcare Services*, aims to help "IT professionals in the healthcare security contexts to establish and maintain Cloud security while selecting and deploying appropriate technical and organisational measures".

The legislative background of cloud services procurement includes, at the EU level, the Network and Information Security Directive (NISD) 2016/1148/EU and the EU Cybersecurity Act; the Medical Device Regulation (MDR) and the Medical Device Directive; and the GDPR, as well as various national legislations in relevant fields. The NISD defines hospitals as Operators of Essential Services and cloud services providers as Digital Service Providers which means that when procuring respective services they both must comply with the Directive security requirements. They also share responsibility for how the health data are stored and processed (assuming roles equivalent to the GDPR's data controller and data processor).

There is a variety of cloud-based services in healthcare, from health information systems (HIS) to office management to telemedicine. When deploying any of them, many challenges arise, from a lack of trust of cloud solutions and a lack of expertise to integration of cloud with legacy systems and data protection issues (e.g. data deletion or encryption). In addition, cybersecurity threats may be posed by natural disasters, supply chain and system failures, human errors and malicious actions, etc.

The report provides three use cases of an EHR, remote care and medical devices, and reviews a reference cloud architecture, factors for risk assessment, and risk mitigation measures. Further on, a number of security measures and good practices are proposed including:

1. Identification of security and data protection requirements
2. Conducting a risk assessment and data protection impact assessment
3. Establishment of processes for security and data protection incident management
4. Ensuring business continuity and disaster recovery
5. Termination and secure data deletion
6. Auditing, logging and monitoring, and others.

Each of these practices are explained and applied to the three use cases.

In conclusion, the report highlights how the COVID-19 pandemic has boosted migration to cloud in healthcare but notes that the majority of cloud services in this sector are still used for administrative and not clinical purposes due to "lack of trust in Cloud services, lack of expertise, compliance requirements, particularly in relation to data protection, and more". By outlining the foundations and good practices of cloud service provision in terms of cybersecurity and data protection, ENISA aims to further accelerate healthcare's transition to cloud-based operations.

Source and image credit: ENISA

Published on : Thu, 25 Feb 2021