Joint Recommendations Brief for Cybersecurity in Healthcare Sector by Horizon 2020

TACKLING CYBER RISKS IN CRITICAL HEALTHCARE INFRASTRUCTURE

A Joint Catalogue of EU Solutions for Cybersecurity in Healthcare

Key steps towards integrating cyber integrity and resilience in critical healthcare infrastructure

Three EU-H2020 projects, CUREX, PANACEA and SPHINX, have established a synergy to foster the integration of cybersecurity in Healthcare Sector. Leveraging their research outcomes, the H2020 projects focus on important aspects identified within healthcare that bring forward the need for regulatory interventions, technological solutions and methods to influence human and organisational factors.

Key Challenges

The Sector lacks cybersecurity culture:

- Legacy systems are used in parallel with the latest healthcare delivery machines, and their communication often relies on outdated and vulnerable APIs.
- The personnel in healthcare organisations usually demonstrate low to medium awareness of cybersecurity practices.

Cybersecurity is not deployed efficiently:

- Often, the healthcare organisations administrations and/or policy makers do not have a clear picture of how to set up cybersecurity systems, as well as the expertise and budget needed for such project.
- Cybersecurity departments are not populated adequately, for example a high-ranking official (e.g., a CISO) is responsible for several different domains and intermediate roles are missing.
- The cybersecurity is not addressed with a preparedness approach, that is the focus seems to be more on reacting to security incidents, rather than preventing them by putting the appropriate solutions in place.

Digitization of healthcare presents risks, apart from benefits:

- The management of the digitized information takes place in a work environment where in addition to an operator and a workstation, there are several medical devices and a patient (and in some cases also the relatives/caregivers), external service providers and even the public. The high turnover of the human factor and undetected vulnerabilities of some devices result to significant cybersecurity risks.
- Healthcare operators are required to comply with cybersecurity measures which they often see as tasks irrelevant to their clinical work that hinder their main healthcare delivery duties.

The HRB - Horizon Result Booster is an initiative funded European Commission, Directorate General for Research and Innovation, Unit J5, Common Service for Horizon 2020 Information and Data.

Capture QRcode or follow this URL

horizonresultsbooster.eu

Joint Recommendations Brief for Cybersecurity in Healthcare Sector by Horizon 2020

TACKLING CYBER RISKS IN CRITICAL HEALTHCARE INFRASTRUCTURE

A Joint Catalogue of EU Solutions for Cybersecurity in Healthcare

Recommendations

Regulatory

- Certification, as a way to pre-emptively test the Information Security status of an organisation and ensure its continuous improvement, should become mandatory, at least gradually.
- Guidelines for including the cybersecurity in the certification schemes of care centers should be adopted by certifying organisations (e.g. the Joint Commission International).
- European level norms (e.g., GDPR) should be updated to provide detailed directions on how to establish cybersecurity practices in healthcare organisations, to prompt regulatory changes in national levels as well.

Technological

- A holistic, supported and validated cybersecurity system should be in place providing healthcare organisations tools such as Security Information and Event Management, Vulnerability Scanning, Intrusion Detection Systems.
- Security-by-design approaches should be established in medical devices' design and deployment and be coupled with compliance verification to increase conformity levels.

Non-technical & Organisational

- Training and cybersecurity awareness should start at education level, involving not only IT personnel but healthcare operators as well, to build habits and processes that incorporate cybersecurity practices and pave the way to apply cybersecurity-oriented rules to limit cyber-risk factors.
- Healthcare top management should be better informed on the modalities of setting up a holistic cybersecurity system, the human and financial resources needed.

Meet the Projects

CUREX

CUREX (seCUre and pRivate hEalth data eXchange) - Enabling secure and authorized sensitive health data exchange. **curex-project.eu**

Grant Agreement No.826404

Panacea

PANACEA (Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people) – an integrated solution for cybersecurity in healthcare covering technology, people and processes. **panacearesearch.eu**

Grant Agreement No.826293

SPHINX

SPHINX (A Universal Cyber Security Toolkit for Health-Care Industry) - Enhancing the cyber protection of Health IT Ecosystem and ensuring the patient data privacy and integrity. **sphinx-project.eu**

Grant Agreement No.826183

The HRB - Horizon Result Booster is an initiative funded European Commission, Directorate General for Research and Innovation, Unit J5, Common Service for Horizon 2020 Information and Data.

Capture QRcode or follow this URL

horizonresultsbooster.eu