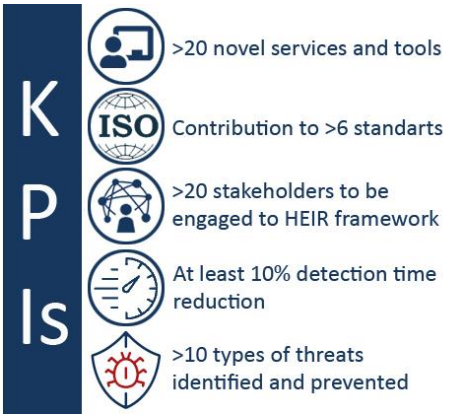
HEIR Newsletter 1

April 2021

In this Issue

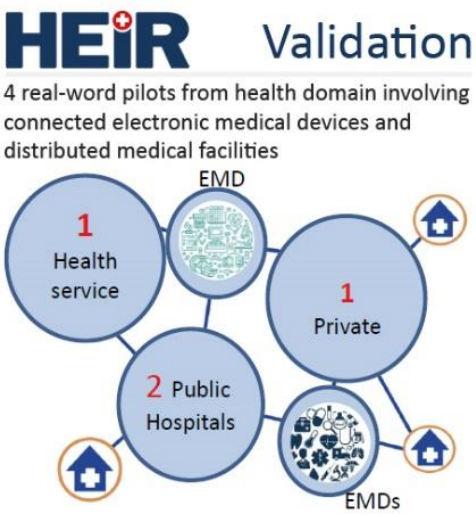
Overview

HEIR (**A Secure Healthcare Environment for Informatics Resilience**) is a European Union project under the H2020-SU-DS-2019 work programme, launched on September 2020. HEIR has 3-years duration and aims at developing a thorough threat identification and cybersecurity knowledge base system both local (hospital/medical centre) and global (including different stakeholders) levels.



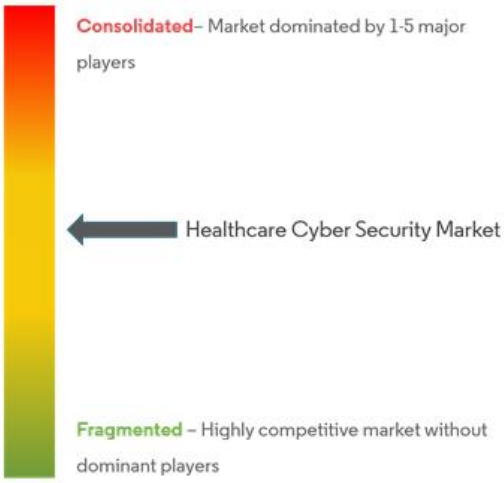
To serve the ambitious objectives, the HEIR framework adopts a modular design that integrates the following functionalities:

- Real time intelligent threat hunting services, facilitated by advanced machine learning technologies, supporting the identification of the most common threats in electronic medical systems;
- Sensitive data trustworthiness sharing facilitated by the HEIR privacy aware framework;
- Innovative Benchmarking based on the calculation of the Risk Assessment of Medical Applications (RAMA) score, that will measure the security status of every medical device and provide thorough vulnerability assessment of hospitals and medical centers;
- The delivery of an Observatory for the Security of Electronic Medical Devices; an intelligent knowledge base providing advanced visualizations for each threat identified in RAMA and facilitating global awareness on EMD-related threats.



Goals

- ✓ Citizens secure access to electronic health records and the possibility to share these across borders;
- ✓ Support data infrastructure to advance research, prevent disease and personalise health and care in key areas;
- ✓ Facilitate feedback and interaction between patients and healthcare providers, enhance disease prevention and empower people take responsibility for their management of their health.



Healthcare Cybersecurity Market Concentration
[Mordor Intelligence, Healthcare Cyber Security Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)]

Cybersecurity Market Trends 2019-20

The increasing number of cyber-attacks and data leaks is the leading factor driving the growth of the healthcare cybersecurity market.

- Global cybersecurity market was valued at USD 149.67 billion in 2019 and is projected to have a value of USD 304.91 billion by 2027 experiencing a growth of CAGR of 9.4% during 2020-2027.
- Healthcare cybersecurity is one of the industry segments of the overall market and is expected to witness the highest CAGR growth until 2025.
- The market is also driven by the changes in the technology surrounding data storage and communication as well as devices for the delivery of telehealth medicine–management of the patient within the home environment.
- The increase in medical data leakage will make the malware & spyware segment go through a 17% growth during 2019-2025.

Issues in Cybersecurity

Issue 1-Healthcare Data Breaches

Healthcare data breaches are a growing threat to the health care industry, causing data loss and monetary theft, and attacks on medical devices and infrastructure.

Issue 2-Vulnerable Medical Devices

As billions of medical devices will be imported into the healthcare domain, the impact is expected to be significant. Despite the evident material gains due to the increased digital connectivity, these technological advancements in the healthcare domain often come with security risks due to their novelty and complexity.

Issue 3-Privacy-Sensitive Data

Despite the wide range of tools and services already available to facilitate the operations in hospitals and medical centers, that domain still lacks innovative, secure execution environments based on novel tools and services that can establish secure digital collaboration.

Issue 4-Legacy Systems

Field-specific challenges (many healthcare systems are in existence within various localities; systems do not communicate efficiently, leading to patients transporting their medical records in paper format between hospitals; records not always available on time and can be easily lost and left open for public scrutiny) impose yet another need for such validated systems in real-life environments, addressing issues of Information Governance and privacy concerns.

Issue 5-User Awareness

Security policy, governance and end-user awareness need to extend across all processes and levels of healthcare environments as complex systems become more and more interconnected.

Issue 6-Trust Increase

Cyber-crime and attacks against critical infrastructures affect the economy and business growth in multiple ways. Achieving a high degree of trust in EU digital networks, products and services requires multidisciplinary research on longer-term security challenges complemented by non-technical aspects of cybersecurity and digital privacy such as business viability and business alliances and collaborations.

Regional Growth of Healthcare Cybersecurity Market (2019-24) [*Mordor Intelligence, Healthcare Cyber Security Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)*]

The increasing number of cyber-attacks and data leaks is the leading factor driving the growth of the healthcare cybersecurity market. The value of medical data being leaked or stolen as well as the limited security measures in place are causing this increase. The market is also driven by the changes in the technology surrounding data storage and communication as well as devices for the delivery of telehealth medicine – management of the patient within the home environment. A prime example of that was seen in the rising demand for cloud services, especially during the COVID-19 pandemic as well as the expanding use of mobile devices for data storage, transfer and remote monitoring. The evolution of regulations around healthcare cybersecurity has also benefited market growth.

However, there are also factors that restrain the growth of the healthcare cybersecurity market. One of them is the shortage of trained professionals, able to understand and operate the cybersecurity services a hospital or any healthcare facility adopt. This is also related to the lack of awareness around cybersecurity in healthcare. Finally, the high cost of cybersecurity solutions is another restricting factor that slows the growth of the market.

Contact Project Coordinator: Prof. Hervé Debar, INSTITUT MINES-TELECOM, herve.debar@telecom-sudparis.eu
General inquiries: info@heir2020.eu

www.heir2020.eu @h2020_heir HEIR H2020 Project

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 883275.