D1.1

HEIR innovations for healthcare systems

Project number	883275
Project acronym	HEIR
Project title	A secure Healthcare Environment for Informatics Resilience
Start date of the project	September 1st, 2020
Duration	36 months
Programme	H2020-SU-DS-2019

Deliverable type	Report
Deliverable reference no.	D1.1
Workpackage	WP1
Due date	12-2020 – M04
Actual submission date	04/01/2021

Deliverable lead	TUD
Editors	Apostolis Zarras
Contributors	Herve Debar (IMT), Giorgos Spyridakis (ITML), Hara Stefanou, Andreas Raptopoulos, Dimitris Karamitros (WEL), John Chang (CUH), Celia Nilssen (NSE)
Reviewers	Eftychia Lakka (FORTH), Michalis Vakalellis (AEGIS)
Dissemination level	PU
Revision	1.0
Keywords	Cybersecurity, Privacy, Challenges, State of the Art

Abstract

This deliverable sets the scene for the project's work to follow by identifying the role of security in the health domain and gaining insight into the parameters that drive the security, assurance, and privacy in a healthcare system. Moreover, it performs a literature review (academic and technical) focusing on all relevant technologies and defines HEIR innovations against existing solutions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275

Executive Summary

Health is an essential part of Europe's social model, contributing to inclusive growth and social cohesion. In most EU countries, there is an enormous investment of resources into acquiring the latest e-health tools/services and applications to provide the most effective and efficient healthcare services for their citizens. These healthcare services include sharing health information with relative ease, improving the interaction between healthcare professionals and their patients, and making access to the best healthcare services and expertise. Digital health technologies can improve health outcomes by increasing patient engagement in self-care, closing communication gaps, identifying and tailoring services to meet patients' needs with chronic conditions and multimorbidity, and improving decision-making by consumers and health care providers.

Unfortunately, as with most sectors, the digitized healthcare sector also presents increasing risks for healthcare systems/services, arising from malware infecting healthcare systems; cybersecurity of medical devices that employ wireless technologies and software, personal data privacy leakage, leading to compromising of the health information, and safety of millions of people. Therefore, it is clear that healthcare organizations are on the high end of the spectrum when it comes to cyberattacks. Furthermore, experts say that health care lags far behind other industries, like the financial sector, in the way it protects its information technology infrastructure. And unlike finance, a health care failure can end with injury or even death.

In this context, and in line with its project statement, HEIR aims to provide a thorough threat identification and cybersecurity knowledge-based system that will focus on depicting the landscape of cyber threats for the ICT-based healthcare ecosystem, detailed cybersecurity assurance statuses, and their evolution over time.

More specifically, HEIR is expected to create a dynamic health ecosystem incorporated with advanced tools and modules to calculate and measure the risk assessment score of the health sector (EMDs and related subnetworks) and thus offer advanced cybersecurity and privacy risks management in health systems and services. In addition, HEIR will advance state of the art in the fields of *(i)* cyber threats identification, monitoring and protection, *(ii)* data exchange and protection; and machine learning – facilitated threat detection, mitigation, and real-time response; *(iii)* a multiple-level visualization and awareness-raising mechanism. Finally, it will inspect and report on the IT health sector's challenges and requirements through its advanced data aggregation, evaluation, and assessment system.

Towards this direction, this deliverable aims to investigate the critical role of cybersecurity and privacy technologies against the elevated cybersecurity threats and challenges that accompany the potential benefit in the health domain. In essence, this deliverable goal is to set the bar high and ensure the project's progress beyond the global competitive landscape.

Table of Contents

List of Figures

Glossary

ABE	Attribute-Based Encryption
ANIMA	Autonomic Networking Integrated Model and Approach
BAN	Body Area Network
BRSKI	Bootstrapping Remote Secure Key Infrastructure
CA	Certification Authority
CAGR	Compound Annual Growth Rate
CDA	Clinical Document Architecture
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DTLS	Datagram Transport Layer Security
EMD	Electronic Medical Devices
ENISA	European Union Agency for Cybersecurity
EPR	Electronic Patient Record
EST	Enrolment over Secure Transport
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
IAM	Identity and Access Management
IBE	Identity-Based Encryption
ICT	Information and Communication Technologies
IoMT	Internet of Medical Things
IPI	Interpulse Interval
MDR	Medical Device Regulation
ML	Machine Learning
NHS	National Health System
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OSEMD	Observatory for the Security of Electronic Medical Devices
OSSIM	Open-Source Security Information Management
PAM	Privileged Access Management
PET	Privacy Enhancing Technologies
PKI	Public Key Infrastructure
RAMA	Risk Assessment for Medical Applications
SIEM	Security Information and Event Management
SSI	Self-Sovereign Identity
WHO	World Health Organization
ZKP	Zero Knowledge Proof

1. Introduction

The current deliverable, D1.1 – *"HEIR innovations for healthcare systems"*, is the output of the work carried out in Task 1.1 – *"The critical role of security and identity management in healthcare environments"*, which, as planned, was carried out in the first four months of the project (M1–M4). This task materializes the first two of the five objectives of WP1, namely: *(i)* identify the role of HEIR in the security of the health domain and *(ii)* gain insight into the parameters that drive the needs for security, assurance, and privacy in a healthcare system.

1.1 Objectives of the deliverable

The scope of this deliverable is to have an initial document, which covers the critical role of cybersecurity and privacy technologies against the elevated cybersecurity threats and challenges that accompany the potential benefit in the health domain. This deliverable target is to ensure HEIR's progress beyond the global competitive landscape. To achieve this goal and minimize the risk of creating an obsolete HEIR framework, a set of detailed literature reviews (academic and technical) has been carried out on the cybersecurity and privacy technologies adopted in the Health context. The literature review is focused on all relevant technologies and define HEIR innovations against existing solutions. Health and Medical-related cybersecurity challenges and requirements have been identified to ensure that the proposed solution is following today's trends. Finally, a short survey is also carried out to identify cybersecurity threats in the health sector as well as mitigation procedures. This survey assisted on a more targeted focus of state-of-the-art solutions described in Section 5.

1.2 Structure of the deliverable

The deliverable is organized as follows:

- Section 2 presents the rationale and motivation behind the HEIR efforts.
- Section 3 sets the scene providing important background information on the cybersecurity of medical devices.
- Section 4 then highlights the challenges that have been identified when assessing the implementation of HEIR in the context of medical devices' attacks and defences.
- Section 5 provides a comprehensive analysis of the state-of-the-art, highlighting projected advances both for the HEIR platform as a whole and for each specific scientific and technological domain of interest.
- Finally, the concluding remarks, including a sketch of the way forward, are presented in Section 6.

2. HEIR rationale

2.1 The need for the HEIR platform

The health sector is steadily becoming the de facto target for cyberattacks. Based on the most recent ENISA report at the end of 2018 [1], cybersecurity incidents have shown that the healthcare sector is one of the most vulnerable. On average, US healthcare facilities have been victims of one cyber-attack per month, and half of them *"have experienced the loss or exposure of patient information during this same period (26% of the other half is unsure)"*. This phenomenon can be explained by combining two factors: *(i)* the high value of healthcare facilities' assets and *(ii)* the ease with which they can be compromised. Medical data is *10-20 times more valuable than financial data* since healthcare records can continue to being exploited even after resolving the security breach that released them. Simultaneously, the healthcare industry is behind other industries in protecting its infrastructure and data. As a matter of fact, Trend Micro conducted a study using Shodan [2] – a search engine that indexes internet-connected devices – and found over 100,000 records relating to medical equipment and hospital computers worldwide that are openly exposed and potentially vulnerable to attack.

The problem is further exacerbated by the ever-increasing value of the health sector: "In 2015, healthcare spending accounted for 8.7 % of GDP in the EU. It could reach up to 12.6 % of GDP in 2060": this then creates an even more tempting target for miscreants [3]. In a recent speech about the Digital Single Market, Commissioner King stressed that: *"...ensure that those tens of billions of new products are sufficiently cyber-resilient – both before they are put on the market and beyond, as new threats emerge"*. Towards this end, the European Commission has identified three challenges related to healthcare systems: *(i)* citizens' secure access to electronic health records and the possibility to share these across borders, *(ii)* support data infrastructure to advance research, prevent disease and personalize health and care in key areas, and *(iii)* facilitate feedback and interaction between patients and healthcare providers, enhance disease prevention and empower people to take responsibility for the management of their health. Focusing specifically on *Electronic Medical Devices (EMD)*, these suffer from numerous and multi-layered vulnerabilities. Default, weak or no password authentication for remote connections, unencrypted traffic or obsolete and insecure cryptographic algorithms, unsupported operating systems, outdated, unmanaged and vulnerable software are among the most severe problems that jeopardize both their smooth operation and the data aggregated and stored. At the same time, device malfunctions can cause inappropriate or ineffective treatment or more severe consequences. For example, if a patient's pacemaker gets hacked, it could malfunction and send electricity to the person at the wrong times, leading to serious injury – or even death.

Having these challenges as driving forces, European regulators have already started to act against the enormously growing cybersecurity risks associated with the healthcare sector by introducing cybersecurity requirements for devices, systems, and infrastructure in various regulatory frameworks, addressing both the healthcare sector specifically and the industry horizontally. Europe's health sector cybersecurity framework includes the following regulators/directive: The new *Medical Device Regulation (MDR)* that enters into force in May 2020 introduces new General and Safety Performance Requirements for devices' security. The Directive on Security of *Network and Information Systems (NIS)* entered into force in August 2016 and had to be transposed into the Member States' national law by May 2018. The *General Data Protection Regulation (GDPR)* entered into force in May 2018 and introduced stricter rules on processing and transferring individuals' personal data in the EU. The forthcoming Cybersecurity Act provides for a European cybersecurity certification scheme. The HEIR consortium believes that the security measures cannot be addressed from an isolated viewpoint:

thus, also in compliance with all the above-mentioned regulations/directives, HEIR will contribute to the recognition that a single electronic medical device/network/system will need to implement security features that originate from multiple regulatory frameworks (MDR, GDPR, ENISA, NIS). As such, to boost the overall level of digital health security in Europe, HEIR will attempt to set up a broad European network for establishing good security practice in all regulatory frameworks to reduce market access limitations, conflicting requirements, and unnecessary administrative burdens.

2.2 General objectives of the HEIR

The HEIR project includes objectives of a general nature as well as specific objectives explored within the remit of this project. In this section, we outline concisely the objectives of the general nature, which serve in an overarching and complementary manner to the specific objectives.

Objective 1: Develop and support a threat identification and cybersecurity knowledge base system that supports trustworthy data exchange across the healthcare supply chain, threat prevention, detection, mitigation, benchmarking, and certified assurance. Validate, demonstrate, and perform an experimental evaluation of the proposed framework on four real-world healthcare scenarios.

Objective 2: Provide scientific and technological advances in Risk Assessment and Security in the context of interconnected health devices, including technologies on cyber-security and protection, vulnerability assessment and benchmarking mechanisms, (distributed) machine (deep) learning and anomaly detection, data management and information control, and privacy-aware framework, which are orchestrated and leaned towards the comprehensive cyber-intelligence framework for healthcare systems.

Objective 3: Provide novel tools and services for enabling secure data storage and sharing in healthcare operations, leveraging innovative, secure execution environments, novel mechanisms related to security, privacy, accountability, and trustworthiness, that will offer effective means for digital collaboration and data exchange, malicious and anomalous behaviour detection, and trustworthiness intelligence awareness for the EU healthcare ecosystem.

Objective 4: Facilitate a secure exploration of HEIR's full potential in the EMD ecosystems and the wider healthcare environments and realize societal and industrial opportunities by validating the HEIR framework in real-world settings via complementary use cases driven by large healthcare practitioners.

Objective 5: Consolidate international and European links, raise awareness, collaborate with standardization bodies, facilitate standardization of security assessment, and ensure the technology transfer of project's results.

Objective 6: Boost the effectiveness of the European Security Union in the domain of EMD and healthcare services by offering high TRL solutions (TRL 6-7) and by ensuring business continuity and long-term sustainability during and after the project lifetime.

2.3 Threat identification and cybersecurity knowledge system

Within all industries, technology plays a crucial role; healthcare is one of the most important. Information technology and electronic medical devices have significantly impacted health services provision worldwide, and at the same time, achieved a significant shift in the manner of thinking about cybersecurity.

High demand for patient information and often-outdated systems are among the primary reasons healthcare is now the biggest target for cyber-attacks. Private patient information is worth much

money to attackers making the industry a growing target. Confidential patient data needs to be accessible to staff, both on-site and remotely, and on multiple devices. The typically urgent nature of the medical industry to be able to share information immediately entails many risks. According to the ITRC Annual Report 2019 [4], the Medical/Healthcare sector exposed the second-highest number of sensitive records, revealing a total of 39 million (39,378,157) records, and exposing the lowest number of non-sensitive records (1,852) for the year.

It is beyond dispute that the health sector has become increasingly technology-dependent, but as the number of connected medical devices continues to rise, so does healthcare organizations' attack surface. Medical devices are an easy entry point, and health organizations must deal with thousands of medical devices connected to their network, each acting as a potential threat for attackers. With the growing dependence on electronic medical devices, attacks targeting them will become an increasingly common phenomenon.

Although the healthcare environment had always been a target for cybercriminals, recent data indicate the magnitude of healthcare problems nowadays. According to the *World Health Organization (WHO)*, the number of cyberattacks launched has increased five-fold during the COVID-19 pandemic [5], and health care organizations have become prime targets. Cyber threats have been increased as a result of malicious cybercriminals aiming to take advantage of the pandemic.

Under these circumstances, healthcare organizations need to place cybersecurity on a higher pedestal than it has been in the past or face severe consequences for themselves and the patients they serve. Considering this, a rising number of health organizations are currently more willing to leverage cyber threat intelligence to be fully aware of their institutions' cyber threat situation. The first step in tackling these challenges is for healthcare organizations to understand the cybersecurity vulnerabilities already present within their networked medical devices, including the potential exposure of sensitive information and the associated privacy issues. And obviously, increased awareness of cybersecurity and privacy issues within the whole healthcare ecosystem should not be omitted [6].

HEIR responds to that challenge by providing a comprehensive solution offering threat identification services and at the same time acting as a knowledge base on two levels of interest: the first within the boundaries of a healthcare organization and the second including different kinds of stakeholders worldwide. This will be achieved through one single platform providing an integrated set of services such as a privacy-aware framework, innovative benchmarking mechanisms based on *Risk Assessment for Medical Applications (RAMA)* scores and forensics technologies, combined with data sharing capabilities between a large number of institutions in the health sector.

The integration of the HEIR platform includes various components, which are interdependent and necessary for successful threat identification and creating a cybersecurity knowledge system. This will result in the successful provision of the envisioned services, which will be the four pillars of the HEIR framework, as shown in Figure 1, combining real-time threat hunting services, sensitive data trustworthiness sharing, benchmarking based on the calculation of the RAMA, and an Observatory for the security of Electronic Medical Devices we will have to achieve to provide a holistic cyber-intelligent platform to enhance the security level of healthcare environments.

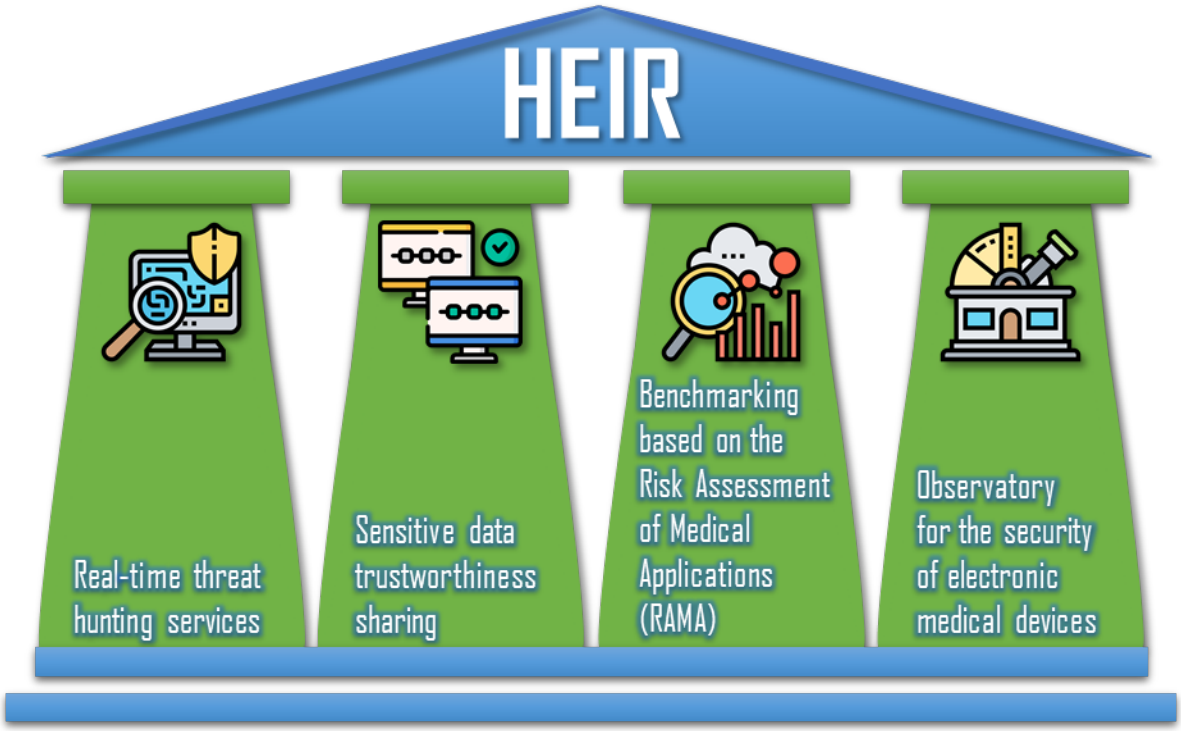

Figure 1: HEIR framework pillars

To accomplish the pillars mentioned previously, the HEIR architecture rationale is based on a multi-layered hierarchical structure. The HEIR baseline consists of two technology facilitators: *(i)* an intelligent threat monitoring and hunting module facilitated by advanced machine learning technologies and *(ii)* a privacy-aware framework enabling trustworthiness in sharing sensitive information. These two essential parts of the solution will allow real-time threat hunting and ensure the secure flow of data in full agreement with the European legislation (GDPR). The information produced by the facilitators will then be imported to the HEIR core framework comprising the main services offered by the solution.

Modularity, a key feature of the HEIR solution, will make the framework applicable to a wide range of healthcare environments, from the simplest to the more complex. Furthermore, its extended capabilities will be necessary to support new types of threats and provide the respective recommendations to the users. This attribute will boost the commercialization potentials of the HEIR framework as different business ecosystems will take advantage of HEIR services.

A more detailed description of the solution with respect to its four main aspects of the HEIR platform follows.

2.3.1 Real-time threat hunting services

Identifying threats in the healthcare organization is a considerable challenge. Electronic medical devices and operational technology cannot easily be secured or upgraded, leaving the organization and its patients always vulnerable. Healthcare organizations, and hospitals, in particular, are vulnerable because, generally, their networks are not well protected, and their data is valuable.

According to IBM Security Cost of a Data Breach Report 2020 [7], companies that had fully deployed security automation technologies, which leverage machine learning and automated orchestration to identify and respond to security events, experienced less than half the data breach costs compared to those who didn't have these tools deployed—$2.45 million vs. $6.03

million on average. That report also indicated that the average cost of a data breach in the healthcare industry is $7.13 million, which means an increase of 10% compared to the 2019 study.

Given the circumstances, threat-hunting services are considered essential for the health sector. Their contribution is extremely beneficial. Their results include a reduction in breaches and breach attempts, a smaller attack surface with fewer attack vectors, an increase in the speed and accuracy of response, and measurable improvements in the security of the environment.

An integral part of the HEIR framework is the intelligent threat monitoring and hunting module to provide threat detection as a service. The HEIR intelligent threat hunting module monitors all valuable assets/resources, performs advanced predictive techniques to identify vulnerabilities and threats in real-time, supported by novel machine learning models for anomaly detection and threat classification. It comprises Security Information and Event Management services for real-time critical event classification and forensic/ threat visualization services combining individual security elements by applying state of the art *Machine Learning (ML)* techniques and Advanced Visualization.

The indispensable function of monitoring the underlying health systems and analyzing in real-time the vulnerabilities of them will be this tool's upper goal, which will be able to monitor the complex health infrastructures efficiently and analyze them for different threats. This tool consists of two modules. Through the first one, the *Security Information and Event Management (SIEM)* services will be implemented. The second one will utilize ML models and will provide forensics visualization services. It is expected that novel ML that will be developed, as well as existing ML models appropriately adapted to match the requirements of the Health system, will be utilized to match the requirements of the Health systems. It will report intelligent real-time security, privacy, and data protection warnings to all stakeholders in the healthcare ecosystem, and it will utilize the forensic module.

HEIR real-time critical event classification component will act as the core SIEM service by receiving data streams from the different HEIR modules and, consequently, performing data classification based on specific rules related to cybersecurity requirements and cyber-threats' level of criticality. The module will allow the processing of increasing amounts of data and adding the possibility of event correlation at different layers with more complex rules. The data collection is done on the monitored infrastructure by SIEM Agents, and the events are sent to the SIEM engine core, where they are processed and correlated. The events gathered, as well as the alarms generated, and the configuration used is integrated with the *Open-Source Security Information Management (OSSIM)* deployment in the SIEM for its storage and visualization.

In forensics work, "best practice" dictates that every piece of evidence is collected. But this can result in massive datasets and cause important details, associations, or trends to be missed. The HEIR incidents' identification & visualization module is a set of tools that allow datasets to be viewed graphically and combined with other datasets to improve the investigator's understanding and identify possible problems in many scenarios, including healthcare operations. The module will augment and facilitate the "after the fact" analysis of digital forensic evidence, fed by the Real-time critical event classification module, by providing different ways to visualize data collected by IT personnel during the forensic analysis. This module can also significantly enhance the analysis of data while the illegal activity is ongoing. This is possible by enabling the investigator to easily gain situational awareness by offering a visual overview of the system, where data that might seem normal when examined individually might be combined with other data and reveal patterns or correlations between them, which could identify security threats.

The edge-deployed framework will be responsible for collecting the minified data from the monitored devices' deployed agents and providing live feedback to the event controller. This controller will provide the necessary information to the Event Analysis dashboard that provides a real-time and a timeline analysis through pre-configured views as well as gets feedback from a threat-response module. The threat response module is responsible for gathering info about potential threats and employing human feedback from IT security experts and evolving ML algorithms to provide actions or suggested actions. The intelligent threat hunting procedure is split into three levels. The first-level analysis includes agents installed in monitored devices and the collection of various metrics. The second-level analysis deals with the HEIR SIEM engine, an integrated monitor device that applies edge computing with local intelligence to monitor the raw data at customer premises, performs data reduction, and runs adversarial ML techniques. An IT security expert team will perform the third-level analysis by investigating the alarms and events and make deductions on the appropriate responses and actions to be followed. The security expert is fully supported by ML and visualization subsystems to raise his situational awareness and drill down to available data. Based on the security expert analysis, the ML subsystem is constantly trained and improved. The technical architecture is shown in Figure 2, including the frameworks utilized to deliver a seamless, all-inclusive solution for intelligent, real-time threat hunting.

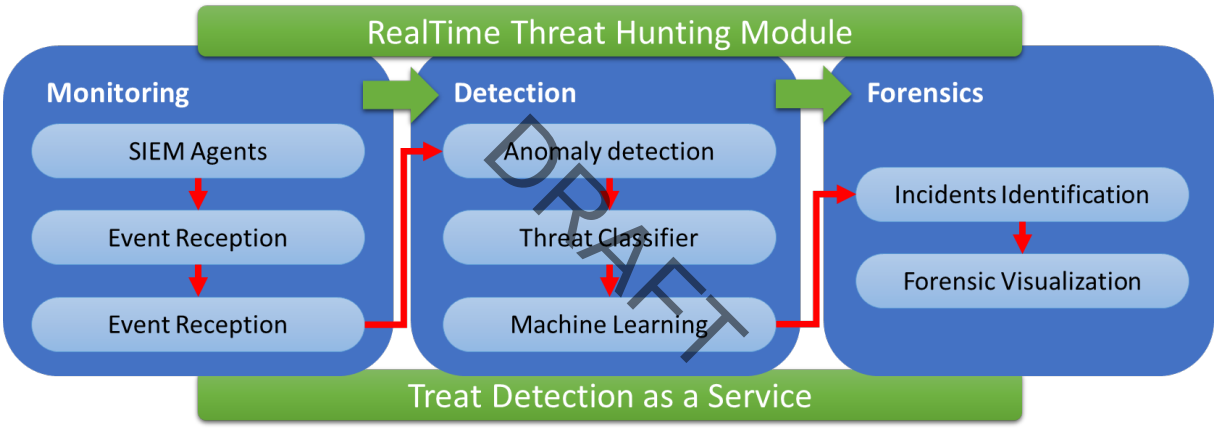

Figure 2: Real-time threat hunting module

The service is accessed through a responsive web interface. The agents deployed on different critical monitored resources are collecting with the less intrusive way data from the monitored resource, allowing configuration for less invasive monitoring or almost real-time data collection, allowing for early threats identification in the most critical resources. Apart from collecting the data, the agents provided pre-process it to reduce the need for large amounts of data to be transferred – anonymized – over the network. Data is gathered to security and data analytics tools in order to extract all the valuable information and deliver it to the central Security Centre User Interface.

2.3.2 Sensitive data trustworthiness sharing

The ability of different information systems, devices, and applications to access, exchange, integrate, and cooperatively use data in a coordinated manner, within and across organizational, regional, and national boundaries, is critical in the health sector. The efforts to provide timely and seamless portability of information will not only optimize the health of individuals and populations globally, but will help organizations share best practices to enhance their security posture.

Secure healthcare data sharing options have the potential to benefit healthcare organizations significantly, but entities should understand the challenges of interoperability, as well. Researchers are still looking for ways to develop such a system to enhance patient care while keeping data secure and complying with European and national legislation. Their efforts include secure health data exchange architectures, application interfaces, and standards enable data to be accessed and shared appropriately and securely across the complete spectrum of care, within all applicable settings and with relevant stakeholders

Under the challenges introduced by continuously updated GDPR requirements, the growing exploitation of IoT-based medical devices and wearables, and in an effort to enhance patient care by keeping their data secure, HEIR is aiming to provide novel tools and services to enable secure data storage and sharing within healthcare operations.

The HEIR privacy-aware framework (Figure 3) is to be implemented to meet the challenge of providing trustworthiness in the sharing and processing of sensitive healthcare data. Based on on-going research on the technology brought in by IBM, the framework will offer effective means for digital collaboration and data exchange. Its main contribution will be to add a data-protection layer by decoupling the data processing logic from data access logistics, access control, privacy, governance, and compliance control. By providing isolation, the collaborative privacy-aware framework will allow an untrusted application code from one organization to be executed on another data controller's data without exchanging the data and, therefore, losing control over it. It will primarily hold metadata that would allow for the non-repudiation and integrity of the relevant data sharing agreements and data processing functions, thus ensuring trustworthiness and accountability among the stakeholders involved, even at a cross border setting.

This framework's concept is to manage data sharing and data processing based on a contract. This contract will contain identity and authorization information, enabling the prevention of data leakage and at the same time, providing access control. The contracting mechanism will enable managing data-sharing agreements between parties, including the purposes for which data would be used. At the same time, it would monitor both the ingress and the egress of the applications in a way that enables the provisioning of data quality assessment and sanity checks, respectively. Finally, the adoption of a purpose-based data obfuscation approach will ensure that only the necessary data and level of specificity is provided. The smart contracts will define in a very safe way whom the data belongs to, who can process them, and allow for efficient/safe data sharing and processing.

Auditing capabilities of transactions should not be omitted, as it will provide a valuable tool to regulatory and controlling to regulatory and controlling health organizations as well as to *Computer Emergency Response Team (CERT)* authorities in cases of security incidents or fraudulent actions. Furthermore, permanent and tamper-proof recording of all data related activity will also provide end-users with a complete view on who accessed their personal data and for what reason, and consequently, give them full control of their sensitive information.

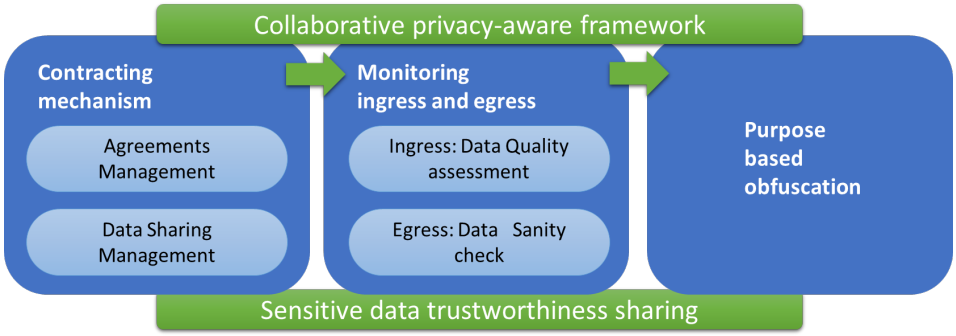

Figure 3: Sensitive data trustworthiness sharing

2.3.3 Benchmarking based on the Risk Assessment of Medical Applications (RAMA)

Scoring and Rating: Like all *National Health Systems (NHS)*, the specifications of medical applications are governed by NHS Digital guidance and set standards are agreed centrally. If the medical application meets these specifications, then the use of the system is decided by the local trust. Trusts themselves do not carry out formal benchmarking on the Risk Assessment directly. This is done by the third parties, based on NHS Digital specifications.

Direct attack on medical devices: To date, there have been no publicized attacks on the NHS's medical devices. In academic circles, it is recognized that such attacks are potentially possible if the device is open to the Web, either via Wi-Fi, Bluetooth, or LAN lines. As most NHS devices stand-alone and reside within the NHS building, access is very limited. That said, it would be prudent if such risks can be addressed. In this regard, the use of Firewalls and device monitoring, an aspiration of the HEIR project, would enable this risk to be further reduced. Again, no formal Risk Assessment currently exists for the use of such devices within NHS sites.

Almost 80% of cyber-attacks are due to Privileged Access Management, whereby the malcontent increases or obtains an administrator account setting to gain entry into the healthcare systems. As the NHS uses both named user accounts, tokens, and passwords, there is some mitigation against such risk. In the past, no formal Risk Assessment has been set as a benchmark: however, NHS Digital has now introduced self-assessment of risk, and it is hoped that all Trusts would be adherent to the revised standards in the future.

2.3.4 Observatory for the security of electronic medical devices

Proactive information sharing about attacks and defensive mitigations builds resilience across organizations participating within a given trust community, evolving herd immunity against attacks that others have seen within their own networks. In the information security world, which is constantly evolving, it is increasingly important to keep up with the latest information security news, threats, vulnerabilities. This knowledge should become an integral part of all security tools that help organizations identify what could be wrong to either avoid or remedy relevant risks. As such, this knowledge is a core part of any security tool's intelligence and resides in the so-called security knowledge bases.

The *Observatory for the Security of Electronic Medical Devices (OSEMD)* will serve as a global monitoring framework for healthcare informatics. It will be a cybersecurity and resilience benchmarking tool for medical IT devices, networks, and computer services. It will act as a public repository for best practices and solutions towards healthcare cybersecurity, enabling healthcare stakeholders to safely access, monitor, and share information about HEIR good practices and mitigate the identified challenges, problems, and vulnerabilities.

OSEMD will be an intelligent knowledge base in the form of a web-based platform. Its function will be to collect, analyze and correlate the results of all tests run by the HEIR Client in any

device or system and give access to that data to a wide range of stakeholders coming from both inside and outside the healthcare ecosystem. This platform will focus on depicting the landscape of cyber threats for electronic medical devices, detailed cybersecurity assurance statuses, and their evolution over time. Insights will be provided about the sectors that require further attention and the level of security provided in the medical devices via interactive graphs and raise awareness to the health services ecosystem on EMD-related threats. The vision is to underline cybersecurity issues common in the healthcare sector and pinpoint interesting outlier values that require further attention. Finally, it will regularly publish the best practices and recommendations based on the analysis of the collected data and display the participating organizations' current security status in terms of adaptation of good practices.

For each threat identified in Risk Assessment of Medical Applications, a large amount of statistical data will emerge after it has been anonymized. These data will be analyzed, and the outcome of these analyzes will be fed to the envisioned Observatory with the support of advanced, interactive visualization tools to extract the cybersecurity and resilience benchmark score of the whole organization. This result will be compared to the global trends documented by other organizations facilitating global awareness of health-related threats.

The HEIR Observatory will provide various statistical indicators to describe the Medical IT Security trends based on the information received by the HEIR Clients. The Statistical Analysis component will compute the appropriate indices and metrics that best capture the adoption of the necessary security practices and measures. Further to that, it is important to identify possible incidents that indicate serious deviations from the expected standards. An Outlier Detector will be integrated into the HEIR System to highlight these cases and present timely notification if needed. Finally, an Artificial Intelligence module will be responsible for predicting correlations between security practices and identified vulnerabilities. New innovative methodologies will be designed to experiment with the possibility of identifying bad security practices and cyberthreats using AI algorithms.

OSEMD concept lies in HEIR Client's connection to the HEIR Observatory, acquiring the latest average statistical data and combining the locally observed scores with the global averages. Through this procedure, HEIR will facilitate the process to benchmark the security of the implemented IT security measures with respect to all measured systems' average. Obviously, the functionality and services offered by the HEIR Client are complemented by the ones provided by the HEIR Observatory.

As an outcome from the monitoring of cybersecurity trend development, customized graphs that compare the outcome of the local achieved scores to the full dataset composed from the input from all collected test results. This process's sole function is for the HEIR Observatory to generate the local/global comparison graphs and benchmarks for the medical providers that participate in the HEIR ecosystem. In addition to that, the HEIR visualizations will be accompanied by basic recommendations and best practices to mitigate the challenges, problems, and vulnerabilities identified.

The envisioned HEIR's global Observatory will raise pan-European awareness regarding health environment cybersecurity and serve as a global monitoring framework for healthcare informatics. It will be a cybersecurity and resilience benchmarking tool for medical IT devices, networks, and computer services and, at the same time, a public repository for best practices and solutions towards healthcare cybersecurity. In a nutshell, the HEIR Observatory, a publicly available knowledge repository and a monitoring service for cybersecurity issues in the medical sector, is the easiest way for both technology literate and illiterate employees in the healthcare sector to examine and understand the information provided by HEIR.

3. Setting the scene

3.1 The cybersecurity of medical devices and the link to HEIR

The healthcare market in the EU, including the technology associated with it, is highly regulated. This is a consciously implemented political reality, reflecting a cultural consensus among European societies, states and institutions; furthermore, Europeans are still resisting the extreme commercialization of healthcare as it is instituted in other parts of the world, with the US as the prominent counter-example, despite the latter's regression towards a more social-conscious provision of healthcare the last two decades. Proceeding to numbers and financial value, as reported in the latest study by *Global Market Insights* [8], within the next five years, the digital health market is expected to grow with a *Compound Annual Growth Rate (CAGR)* of almost 16%, which means it will double by 2025 to a size of 440 billion US Dollars, with data and regulation being fundamental driving forces of growth. Increasing demand for lowering healthcare services' costs by implementing healthcare IT networks will foster industry growth in the future. It is obvious that the implementation of healthcare IT services reduces errors in processes and manages the data efficiently, thereby lowering overall healthcare service cost. The factors mentioned above will propel the healthcare information technology market growth in the future.

Regarding the market segmentation, the digital health market reached 206 billion U.S. dollars in 2020, driven mainly by the mobile and wireless health market [9]. As we are just scratching the surface of the so-called "digital transformation" of health care, it is already evident that a pattern is starting to take shape: "Digital" primarily concerns the creation and management of excessive valuable big data. Healthcare data incorporate even more value, referring to individual human beings' existential and physical attributes. As with all data, they become more valuable when circulated and shared through networks, going, in other words, "online". The cybersecurity market size was valued at $104.60 billion in 2017 and is projected to reach 258.99 US billion dollars by 2025, growing at a CAGR of 11.9% from 2018 to 2025. In fact, the healthcare segment is projected to exhibit the highest CAGR growth of almost 15% during the period 2017- 2025 [10].

Governments of various countries are taking initiatives to encourage the use of secure digital healthcare systems, as these systems help reduce healthcare costs and maintain the quality of healthcare services. Notably, in Europe, EU member states (through the initiatives of respected EU institutions, like the EU Commission) have outlined the eHealth Network [11] to promote cross border healthcare across the EU space. One of the eHealth networks' primary objectives is to enhance interoperability between national digital health systems in exchanging patients' data in ePrescriptions [12], patient Summaries [13], and electronic health records.

Considering the general context of healthcare technology, the ongoing digital transformation, and the challenges that emerge, mainly around the generation and the proper management of sensitive yet valuable, online medical data, we can draw a basic yet very representative outline of the potential for cybersecurity frameworks and initiatives, aimed towards the digital healthcare ecosystem, in our case, HEIR. The Digital Secure Health industry in Europe represents a promising and actively developing sector. However, it is still a young field with a host of challenges and problems, and it is at a low level compared to the USA due to the low level of investments in eHealth. Looking more widely, there are opportunities for genuine transformation and innovation in the health care system, and the EU still has much to do. In this respect, HEIR aims to boost innovation in a secure healthcare system by increasing the quality of various healthcare services and reducing the related costs. It will offer an attractive opportunity for PEs/SMEs firms to increase their European healthcare market presence.

In a nutshell, HEIR will enhance growth and competitiveness in the implementation of cybersecurity-related initiatives in the healthcare sector; it will strengthen the innovation capacity of both healthcare institutions, based on the advanced services offered at a pan-European level, and the cybersecurity services' providers, through the ability to provide services through a centralized healthcare channel.

3.2 Methodology

As Section 2 has already stated, HEIR aims to provide a thorough threat identification and cybersecurity knowledge base system addressing both local (in the hospital/medical center) and global (including different stakeholders) levels, that comprises the following pillars (Figure 1):

a) ***Real time intelligent threat hunting services***, facilitated by advanced machine learning technologies, supporting the identification of the most common threats in electronic medical systems based on widely accepted methodologies such as the OWASP Top 10 Security Risks [14] and the ENISA Top 15 Threats [15].
b) ***Sensitive data trustworthiness sharing*** facilitated by the HEIR privacy aware framework.
c) ***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.
d) The delivery of an ***Observatory for the Security of Electronic Medical Devices***; an intelligent knowledge base accessible by different stakeholders, providing advanced visualizations for each threat identified in RAMA and facilitating global awareness on EMD-related threats.

To realize the aforementioned pillars, HEIR will design and deploy an *Electronic Medical Devices Cybersecurity Framework* that will facilitate intelligent threat identification and hunting services leading to the delivery of the envisioned RAMA. The outcome of these analyses will be available to the IT personnel responsible for the medical devices. More than that, the RAMA client software will submit anonymized statistical data to a central server which will host the envisioned OSEMD. The Observatory will provide statistics for each threat identified in the EMD Risk Index Score through advanced visualization tools. Therefore, the medical IT Personnel and the hospital manager will be able to measure how well the specific hospital or medical center performs compared to average aggregated mean scores. The client will identify outlier values to medical IT personnel, highlight issues which require actions and suggest possible solutions to improve the RAMA and minimize risks. This information will be available via the RAMA client to the IT medical personnel only.

OSEMD will be a web-based platform accessible to stakeholders, scientists, researchers, hospital managers, medical IT personnel, public servants, law enforcement agents, legislators, CERTs and CSIRTs. It will comprise intelligent knowledge-base and interactive visualization tools, and its focus will be on depicting the landscape of cyber threats for electronic medical devices, detailed cybersecurity assurance statuses, and their evolution over time. It will provide insights about the sectors that require further attention and raise awareness to the health services ecosystem. Finally, it will regularly publish the best practices and recommendations based on the analysis of the collected data. The high-level HEIR services and the mapping to relevant tools and technologies are depicted in Figure 4.

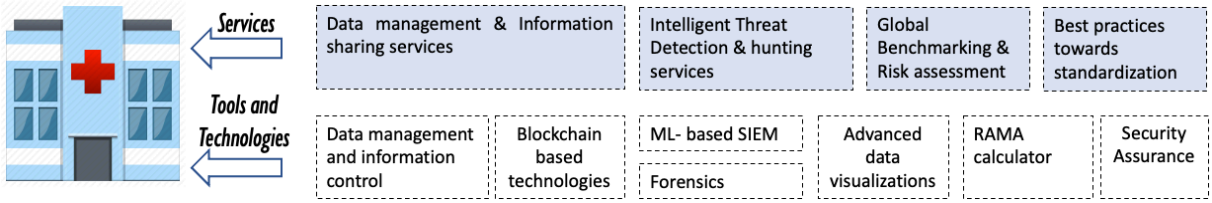

Figure 4: HEIR high-level services and respective tools and technologies

3.3 A snapshot of the offered solution

It is essential, following the presentation of the methodology, to introduce a brief overview of the solution, which will be offered. This will enable the reader further down to be able to link specific challenges that the consortium will need to address in order to achieve the described outcome. In this way, building knowledge on all the steps may facilitate incremental track recording that may facilitate further future work.

HEIR framework is based on a *multi-layered hierarchical architecture*. It comprises HEIR clients, operating at a local level in a wired or wireless LAN in a healthcare facility, providing data for further analysis in the *HEIR Aggregators*. After completing their analysis, they submit anonymized findings to the *HEIR Observatory for the Security of Electronic Medical Devices (OSEMD)*, which aggregates data of all HEIR clients and aggregators and performs detailed data analytics, supported by advanced, interactive visualization tools. The vision is to *(i) provide a detailed analysis of the adoption of suitable technical practices* and at the same time *(ii) underline cybersecurity issues that are common in the healthcare sector* and pinpoint interesting outlier values that require further attention. The information will be presented at different levels (facilitating both general/high level and detailed/low-level visualizations); daily snapshots will also be kept to generate time series of the developments in every aspect of healthcare cybersecurity (see Figure 5).

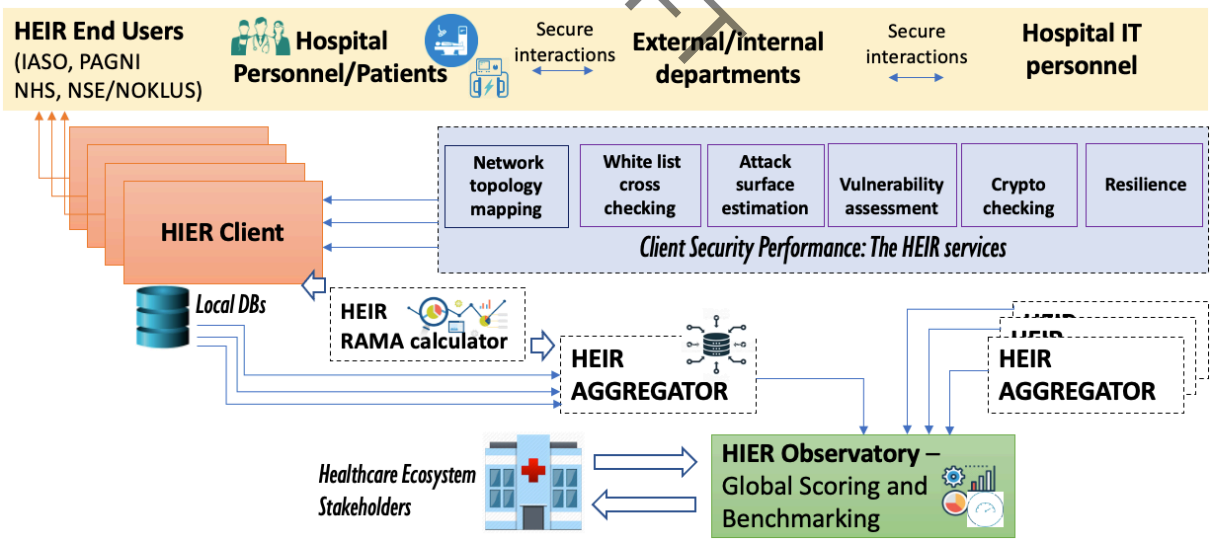

Figure 5: HEIR high-level architecture

The HEIR framework is also *modular*; it can be further extended to support new threats and provide additional recommendations. It can also be modified to support different and more complex healthcare environments. A more in-depth hierarchical architecture is ensured with the provision of HEIR Aggregator. In large healthcare environments as a hospital with many departments, different medical devices, and subnetworks, a single HEIR client may not be enough to support the IT administrators in understanding all the necessary details for every department. The HEIR Aggregator will collect the data from all HEIR Clients, will make the

required evaluations and assessments for each HEIR Client, and finally will provide detailed feedback. Thus, the HEIR Aggregator will be acting as a *"1st level HEIR Observatory"*, assisting the IT personnel to identify which departments in the hospital face critical cybersecurity issues. The HEIR Aggregator will also operate as a *1st level cybersecurity and resilience benchmarking tool*, comparing the cybersecurity status at an intra-organizational level. The aggregated information is further transmitted to the global HEIR Observatory to extract the cybersecurity and resilience benchmark score of the whole organization compared to the global trends documented from other organizations.

3.4 Use-case categories

The four (4) use cases described below (which will also form the basis for the WP6 demonstrations) cover the operational needs of different end-user partners of the project. All of them involve massive amounts of heterogeneous data streams but also illustrate the different yet interrelated application domains of HEIR.

3.4.1 Use-case #1: Privacy enhancement and security information management

Lead end-user: IASO

IASO, one of the biggest women's hospitals in Europe, uses its healthcare information system (including the Laboratory intelligent system (SAP, RIS/PACS, LIS) by integrating and interconnecting all the clinic patients and the associated internal and external doctors/physicians as an entire unit. The hospital owns large medical data concerning women's health and welfare. However, the lack of secure big data management infrastructure restricts the data storage, access, analysis, transfer, and patient/clinician remote interaction. Implementing a cyber-resilient web-based big data management platform is of high importance for IASO information system to boost both the patients' abilities to access their data and the system's capability to control and manage the overall data infrastructure securely and appropriately.

The HEIR framework will enhance the current IASO information system by assessing the hospital's overall security status. More precisely, it will improve the existing health services such that the collected data will be available through a secure platform, interconnected with the SAP LIS, while taking care of security and data privacy concerns. Furthermore, the HEIR Observatory will aggregate the collected data, extract the most important statistical trends on IASO IT security status, and categorized the existing technical risks. This will help the IASO IT personnel identify which departments in the clinic face critical cybersecurity issues and vulnerabilities and address them. The latter will be achieved by providing detailed information regarding the IT configurations with insufficient protection levels and appropriate measures.

In this context, the project will serve as a means of training IASO personnel into security actions and procedures, enhancing their engagement to promote security thinking while improving IASO patients' awareness to handle their data via web-based platforms secure manner.

The main actors of this use case are *(a)* Patients: women, neonates, children (both sexes) *(b)* doctors, nurses, hospital personnel, IT managers, DPO, and *(c)* hospital-related end-users (hospital-related external doctors/personnel).

HEIR will enhance the current IASO information system by assessing the overall security status of the clinic and provide solutions for (i) secure processing of patient data (specializing in women, gynecological cancers, fetal and neonatal health), (ii) vulnerability analysis, (iii) secure communications and firewalls, (iv) big data management and access control, and (v) assisting the establishment of safe and effective networking routes with relevant local and EU hospital institutions to deliver and share big data.

3.4.2 Use-case #2: Boost the security surface of integrated information systems

Lead end-user: PAGNI

PAGNI is using an integrated information system called the OPSI platform. This eHealth IT infrastructure currently links the hospital medical care, the pharmacy, the patient flows, and records. The OPSI's servers are located at the hospital's server room, running services like authentication and authorization (e.g., Role-Based Access Control), relational database management system (RDBMS) hosting, data storage, and middleware's for the communication of OPSI with external systems.

The OPSI platform is an effective mean for the smooth operation and easy management of the PAGNI IT system as the PAGNI's personnel (i.e., doctors, nurses, administrative staff, and the IT department) uses the OPSI platform daily, offering numerous services such as online recording patient's data, ordering of examinations and drugs, payroll processing and logistics, staff accountability, examination order executions. To this end, the main assets that OPSI possesses are patient health records (i.e., examinations, historical data, drug dosages, etc.), visualization of the patient examination results, patient profile, and associated medical data, and IT Infrastructure.

The following subsystems execute the full operation of the OPSI platform: Medical-nursing subsystem (HIS), Administrative-economic subsystem (ERP), Laboratory subsystem (LIS), Medical Imaging subsystem (RIS/PACS), Subsystem of intensive treatment units (ICU), Technical service and biomedical subsystem.

Regarding the OPSI security aspects, the following security features have already been implemented: Role-Based Access Control system, Daily backup of OPSI's data, Software maintenance, Network security practices such as VPNs, Firewalls, etc. However, despite the implemented cyber infrastructure, the OPSI platform is currently facing several cybersecurity and data privacy issues such as malware (including Ransomware) and phishing attempts, unauthorised internal users having access to patient files, External attackers/hackers, mechanical failures, etc., problems with third-party vendors (e.g., issues with the database administrator or cloud provider) resulting in several severe system failures like *(a)* loss of confidentiality (e.g., in the electronic health records), *(b)* loss of availability (e.g., the web interfaces of the OPSI's system) and *(c)* loss of integrity (e.g., clinical records) and so on.

HEIR will enhance the OPSI platform with respect to its data privacy and cybersecurity by measuring and evaluating the hospital IT system's overall security status. In particular, the operation of the OPSI platform will be boosted via the provision of the HEIR vulnerability analysis module, SIEM monitoring tools and forensics analysis, advanced visualization tools, and RAMA calculator. Furthermore, the consortium will install the Blockchain service components and work with the PAGNI team to define the use cases and procedures that are necessary to maintain the distributed health services.

3.4.3 Use-case #3: Secure platform for patients' data exchange

Lead end-user: NSE and NOKLUS

This use case will be structured by joining the two HEIR partners' NSE and NOKLUS forces. It will mainly examine the cross-domain aspect of data exchange between patient representatives (NSE), health data registry representatives (NOKLUS), and researchers (NSE/NOKLUS). The HEIR project will facilitate the secure data exchange and storage as well as the interaction between citizens, research institutions, the Norwegian Diabetes Registry (NOKLUS), and other stakeholders inside a trusted environment.

In this pilot, patient data will be demonstrated gathered on their mobile devices and sensors, and then shared with researchers, the Norwegian Diabetes Registry, and optimally also their clinicians. Data will be made available through a secure platform, providing the stakeholders with patient-gathered data for health service improvement, especially to optimize future consultations, while taking care of both security issues and patients' ability to control their data.

HEIR will prove that utilizing the data from both clinical and personal health systems will provide a better and more comprehensible overview for both researchers, patients and clinicians, and demonstrate that it can improve both the understanding and communication between health professionals and citizen/patient. In addition to providing the equipment and communication for performing this, HEIR will raise awareness for all kinds of users, citizens/patients, and practitioners on the personal security measures that need to be taken. The pilot will provide experiences and measures from testing new ways of using patients' data in a cooperating and data-sharing environment with their researchers, registries, clinicians, and other healthcare services. The patient data involved, will be data from insulin pumps, sensors for blood glucose monitoring, and possibly also physical activity monitoring devices (e.g., FitBit and Xiaomi sensors).

The novel perspectives with patient involvement and engagement and their contribution to clinical decision-making build on the possibility of patients being able to share their data with their researchers and health care personnel, gathered through their mobile devices, including input from various wearable sensors and applications. The general principle is that the clinical practice and decisions will be optimized by having also the patient-gathered data from the time outside the clinic available, for a more thorough analysis. For this to be acceptable for the patient, the system must offer benefits and trust. Data ownership principles need to be addressed if such data is incorporated in the Diabetes Registry, and possible also the clinics' EHR systems, which is a quite new approach and one where there is very little research documentation or experience.

HEIR will work and document a vulnerability analysis of personal health tools and sensors, with respect to issues like secure communications and firewalls, antivirus and antimalware, identity management and access control, SIEM monitoring tools and forensics analysis, IT intrusion detection and access management solutions. It can also provide solutions for encryption, anonymization, access management, and support the patients/citizens' rights for keeping control of their data. Mobile security solutions will ensure that mobile devices' data can be shared on a metadata level, possibly cross-border. Finally, the pilot will test the Blockchain and Discovery service components.

3.4.4 Use-case #4: Blockchain for patients' data and intrusion detection system

Lead end-user: CUH

Croydon Health Services NHS Trust (CUH) is a large integrated organization located in South West London. There are two separate health care systems under one roof in CUH health services: the acute hospital trust and community services, including primary care. With the move to go paperless, the medical records are rendered digital within both domains. At present, this has culminated in two differing electronic systems: Cerner for the acute hospital and EMIS for primary care. In both situations, the end users, namely the clinical teams and the primary care teams, need to communicate with each other: this is being carried out using electronic letters for exchange of data: this exchange of data represents a potential weakness for exploitation by hackers.

CUH IT system has many IT servers, currently hosted by BT, that sits behind the N3 firewall. This firewall is managed by BT such that only authorized users can log into the system, adding

in an extra level of security. The system has its own internal firewalls that are commercially sourced. Within the system, a user name and password are allocated for each end-user, managed by the IT department. These passwords are forced to be updated regularly. Furthermore, policies exist to help mitigate the abuse of user names and passwords. Finally, the actual patient file access in the Cerner system is executed only via special NHS cards.

The current NHS challenges alluded to, are about data security. Since the emails and patient data systems share common servers, and the CUH central system has a web-based presence, then the NHS digital structure is open to abuse: via viruses loaded onto emails by stopping the system from working as in the case of the WannaCry viral attack that caused over £90 million worth of damage and stopped major medical operations, including surgeries from functioning, or by attempted intrusions (hacks) bringing in privacy issues and data leak concerns.

Furthermore, recently the systems are being more linked; thus, more vulnerability spots (both known and unknown) occur. Staying one step ahead of the malcontent individuals or organizations remains key to safeguarding the patient data. In this context, staff education on email and password management via mandatory information governance is one of the many processes on this pathway. However, being human, then these minor issues of forgetfulness or mistakes could culminate in a major breach. As the need for information for patient data/records management is time-critical, the speed of access is also an issue: any secured system has to be flexible enough to ensure that authorized end-users have the correct level of clearance to order tests and view patient files rapidly.

As an acute Trust containing both an Intensive Care unit and a renal dialysis unit in addition to the routine wads and departments expected for any large District General Hospital within the NHS, then we often find critically ill patients are often monitored and managed with in the Trust setting. The machines deployed to deliver and monitor the patient's clinical condition are often web or internet enabled so that data feeds can be utilised wireless via ports. These ports are also available for use for the third parties to conduct maintenance and service, as well as update the software on the machines. As this is an unknown risk, then these ports are often locked down to prevent unauthorised access.

Given the issues raised above, and also being aligned with the recently embarked NHS' security measures, the NHS use-case within the HEIR project would be based on the following two technical investigations: *(a) Blockchain of patients' data.* These files would be tracked to see if the audit trail and erasure could be done and audited to confirm data ownership reliance. If successful, it may be able to demonstrate not only secure access to patient files by authorized end-users but also enable the patient to have ownership and clarity on how their data has been used and, if so, by whom. *(b) Intrusion detection.* The NHS system can be attacked via intrusions and, more commonly, email phishing scams and attachments containing viruses. The WannaCry virus was one such bad attack. With the use of more *Internet of Things* sensor devices, as well as infusion pumps, scanners and complex health care machinery that have ports for service access, then potential threats can arise from hackers getting in via these devices already linked to the healthcare system.

It is envisioned that by implementing the HEIR system on the dummy servers, these planned intrusions can be detected on a simulated ward system to affirm the ability of the HEIR system, utilizing deep machine learning and AI, to mitigate against attacks on the healthcare network that targets the IT ports and the connected devices.

HEIR will boost the Croydon NHS IT system in respect to the (a) secure access/transfer of patient files, (b) patients' ownership of their health data history (c) threat and attacks identification and analysis,

4. Challenges

This section outlines the challenges that have been identified when assessing the implementation of HEIR in the context of the security of medical devices. In particular, the challenges are linked to the core of the solution offered.

4.1 Overview of challenges

Challenge 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. Hospital data security breaches can cost a single hospital a substantial financial fine, litigation, and a damaged reputation. Meanwhile, the health care industry lags other industries in securing its data. In response, health care organizations must invest considerable capital and effort in protecting their systems.

Challenge 2 – Vulnerable medical devices: As billions of medical devices will be imported into the healthcare domain, the impact is expected to be significant. Healthcare providers have a unique opportunity to use the data from these devices to improve patient outcomes. Still, they need to find ways to get insight into so much data so it can be actionable. Medical IoT will extend the connectivity and transmission of health data from the patient to the physician regularly or immediately and continuously in an emergency. The Medical IoT will make medicine participatory, personalized, predictive and preventive (P4 Medicine). 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 its novelty and complexity. As the number of connected devices and cloud networks increases, the attack surface for data breaches or ransomware becomes greater than ever before, and the need for innovative technologies comprising a wide range of fields becomes inevitable to counter such attacks.

Challenge 3 – Privacy-sensitive data: Despite the wide range of tools and services already available to facilitate the operations in hospitals and medical centres, that domain still lacks innovative, secure execution environments based on novel tools and services that can establish secure digital collaboration, especially under the challenges introduced by continuously updated GDPR requirements and the growing exploitation of IoT-based medical devices and wearables. Ethical considerations are playing catch-up: anonymized data sets could be harvested and analyzed without the patient's consent to the use of their data. There is a need for the patient to say how their electronic data can be used and by whom.

Challenge 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.

Challenge 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. Moreover, the lack of security awareness across the environment and fragmented security solutions that don't necessarily work from one system to another (e.g., applying IT resources such as invasive penetration testing and network mapping tools to different departments of medical centres), are major hurdles and roadblocks to exploiting advanced technologies' full potential in interconnected healthcare environments.

Challenge 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.

4.2 Research and innovation regarding challenges

4.2.1 Healthcare data breaches

Data breach refers to the intentional or unintentional release of secure or private/confidential information to an untrusted environment [16]. More specifically, a medical data breach is a data breach of health information, which could include either the personal health information of any individual's electronic health record or medical billing information [17]. Among 3,824 data breach notifications reported between May 2018 and February 2020, 244 (6.4%) is related to the health sector, increasing by a factor of four between 2018 and 2019. Data breach characteristics of the health sector were similar to data breach characteristics of the other sectors. Loss of confidentiality is the most important breach (80.7%) in the health sector, followed by the loss of availability (27.5%); some data breaches are mixed. 175 (71.7%) notifications reported fewer than 300 people impacted. The malicious cause occurred in 58.2% of them, and accidental cause accounted for 25% [18]. These security violations are generally the outcome of other threats endangering the health organizations' ICT infrastructure, including Electronic Medical Devices.

Concerning this great challenge, ***HEIR offers a solution to reduce the detection time of data breaches and increase security monitoring accuracy, which will lead to cybersecurity incident investigations resolved within an acceptable timeframe for the organizations.***

Providing such advanced services is the subject of many innovation initiatives nowadays. It is indicative of the direction cybersecurity is moving that the Innovative Product of the Year - Threat Detection was awarded to IronDome, a Collective Defense platform [19]. A solution that leverages proven analytics, machine learning, and artificial intelligence techniques to identify threats and automates real-time knowledge sharing and collaboration between and beyond sectors to automatically share real-time detections, triage outcomes, threat indicators, and other insights.

Machine learning is changing organizations' approach to threat detection and how they adapt and adopt cybersecurity processes. The idea is not just to identify and prevent threats but to mitigate them as well. An algorithm can learn from its mistakes on the fly. It is always the best version of itself because it is continuously improving its performance. A good ML discipline is one that can "see" patterns of behaviour, guessing the form of an attack and how to fight back. The algorithm can be trained with different types of attacks, learn the methods to gain privileged access and lateral movements, and even adapt in real-time to a situation. An excellent ML approach can learn from false positives. False positives will always exist, but they are reduced with each interaction with an algorithm because the machine is continuously learning. After implementing an ML system, false positives can be reduced by 50% to 90% [20].

Google is an indicative example as it is officially expanding its Chronicle cybersecurity platform into the threat detection realm: by placing ML algorithms into Chronicle, which can then analyze vast swaths of data, this enables the system to identify security threats more quickly – Google has set the wheels in motion for proactive threat detection and alert functionality. At the baseline of the solution, there is also an intelligent data fusion, combining a new data model with the ability to automatically connect multiple "events" into a single unified timeline [21].

A far as secure data sharing between the healthcare entities are concerned, scientists envision safe, collaborative infrastructures. As reported in relevant research [22], such an infrastructure could be based on the blockchain. However, while blockchain is a possible solution to secure the health data of patients, the question is whether the technology is too early in its infancy or if the cost to set up the infrastructure is too high at this moment in time. Of course, the most critical hurdle of all is implementing this technology within the parameters set forth by regulators in the healthcare space. This is a crucial aspect that HEIR will examine.

These are the challenges which ***HEIR also aims to tackle through a threat identification and cybersecurity knowledge base system that supports trustworthy data exchange across the healthcare supply chain, threat prevention, detection, mitigation, benchmarking, and certified assurance.***

4.2.2 Vulnerable medical devices

Recent events have shown the impact of cyber-attacks on infrastructures that we do not expect to fail. The Wannacry incident [23] has demonstrated the increasing reliance on medical devices on classic network and *Information and Communication Technologies (ICT)*. Such technologies, while bringing increased facilities and opportunities, also opens the door to vulnerabilities and attacks. Traditional operation of these medical devices assumed that they would not be accessible from the outside world and would not be connected to the hospital's network. The need to transfer information from the devices to medical files to facilitate care, and the need for these devices to be accessible from the outside world for maintenance, have opened an entirely new set of vulnerabilities. Several research and innovation topics are relevant for this challenge.

Identification and authentication, specifically dedicated to the needs of healthcare personnel. The specific aspects of healthcare operations, such as 24x7 care for patients, increasing use of remote care where you can leave the monitoring devices in the hands of patients (telehealth medicine), emergency situations requiring immediate access without barriers, are usually not well accommodated by classic *Identity and Access Management (IAM)* solutions available today. Healthcare aspects of security policies have been studied in the research literature, but there are no practical implementations available today. Furthermore, organizations tend to rely on well-known tools (e.g., office tools, disk and printer sharing, etc.), where end-users are familiar with the technologies and operators skilled in operating these systems are available. This leads to an additional acceptance and training challenge for the personnel who has to use these new tools.

Definition of monitoring and detection strategies for healthcare networks, complementing access control to highlight anomalous network behaviour. Anomaly detection is hard to establish within healthcare environments, as operating conditions may vary due to the type and complexity of the host institute. For example, EMDs can be placed in patient homes, thus lying outside the classic security monitoring domain. Private "medical" devices are also brought on premises, as well as other equipment such as smartphones and connected watches.

Definition of mitigation strategies. Based on the detected anomalies, the system will deploy flexible network overlays to verify and enforce network activity compliance with security policies. Mitigation remains a difficult topic, particularly with automation, as network management operators are reluctant to let automated processes take the upper hand when dealing with cyber-attacks.

Deployment of these technologies in the context of the cloudification of network infrastructures. Healthcare environments, like others, are moving towards the cloud. This induces a transfer of control from healthcare organizations to external service providers. On

one hand, this may help these healthcare organization get better cybersecurity support. On the other hand, this may create additional difficulties ensuring the protection of sensitive processes and information. Understanding how cloudification of healthcare infrastructures impacts cyber-risk management is a forthcoming important research and innovation challenge.

The medical world is increasingly relying on devices to sense, measure, produce data. These devices are extremely heterogeneous. Some of them, like imaging devices, are large and computationally powerful, but also very expensive and sensitive to ICT-related problems such as loss of connectivity. Other, smaller devices, like heartbeat monitors or blood glucose measurement devices, are remote and can be handled by untrained users. All connected devices forming the *Internet of Medical Things (IoMT)* are extremely sensitive to cyber-attacks. The extreme heterogeneity of end user capabilities is thus an additional challenge, requiring both adaptation of existing technologies, development of new intuitive HMI systems to manage them, increase in the capability of these IoMT devices to defend themselves autonomously, and innovative user training and feedback.

4.2.3 Privacy-sensitive data

New types of pervasive wearable technology bring interesting insights into personal daily life and facilitate various health-related activities. The wearables market growth is stimulated by miniaturization and the development of new types of sensors used by device vendors to create new consumer-level kinds of devices. The gathered data is often transferred to a smartphone-centred ecosystem that provides user-friendly interfaces for visualization, notifications, and further data sharing. Examples of such devices are fitness trackers, smartwatches, smart rings, or smart glasses. Complementary privacy policies are, however, often provided in a hard-to-understand way without clear answers to fundamental questions such as: *"What data is being collected?"*, *"How is the data protected?"* and *"Who has access to the data?"*. Also, since the device's advertised functionality could be based on secondary processing of more primitive data collected from various sensors, it might be difficult for a consumer to relate to all these three privacy dimensions.

By not accepting the provider's data security and privacy agreement, a user is often simply not able to use a full portfolio of the device's features or sometimes not able to use the device or service at all. On the other hand, by accepting it, a user gives consent for various data-transfer activities happening in the background, and often even the ownership of her/his data. Numerous security analyses have been performed to investigate whether wearable devices, smartphone applications, and associated cloud services fulfil the current rules for data security and privacy requirements. Even though these efforts often conclude with alarming findings, this has not yet led to much change in vendors' practice in general when it comes to data security and privacy-related ethical issues, as amassing large volumes of human health data can enable the development of more refined and predictive software which could be further monetarised. Whilst the motive for additional post-processing might not be apparent to the device's end-user at first sight, the uncovered insights provide a potentially compelling advantage over the rest of business competitors in various areas such as targeting advertisement. Therefore, secondary data usage scenarios include data reselling to third-party marketers and insurance companies. Another purpose of this data analysis is usually marketed as product improvement. However, since metadata collection uses additional processing or network resources, it may negatively influence user's experience with the product in various aspects.

As a consequence of this vendor-based user data harvesting, new regulations such as the General Data Protection Regulation (GDPR, implemented in May 2018), have been introduced to *provide increased legal certainty for both individuals and organizations* [24].

After introducing GDPR, it is now common to see applications integrating an explicit user-adjustable set of options dedicated to data collection related settings. This is usually hard to understand and adjust by the common user, resulting in it being generally ignored by the user choosing "select all" or similar – not knowing what (s)he is accepting all these blanket consent options. Recently, multiple companies have provided options to give end-user consent (opt-in) or withdraw (opt-out) for the purpose of further analysis.

Interestingly enough, the existence of regulations such as GDPR enforces regulatory compliance and, indirectly, influences the technology stack behind the technical solution. For example, GDPR-incorporated right to erasure, which is also known as 'the right to be forgotten', essentially imposing design update of distributed Blockchain platform to address all of the GDPR concerns fully.

Based on the described development in this area, multiple challenges need to be continuously addressed:

- coherent way of presenting and interpreting privacy policies to the end-user,
- developer's guidance on implementing opt-in/-out option in various applications, in a way that is easy to relate to for the end-users,
- up-to-date framework that describes technical prerequisites in relation to current regulatory requirements,
- user-friendly ways for users to access, manage, and delete their health data.

4.2.4 Legacy systems

In 2015 the UK NHS committed to migrating from paper records to *Electronic Patient Records (EPRs)* by 2020. All hospitals should comply with the aforementioned direction. For instance, Croydon, as an integrated health care system, with links to Primary Care, via Co-ordinate My Care means that Croydon NHS Trust needs to be able to integrate primary care records to EPR. This is a major problem given that the Primary care systems operate using different medical applications. Beyond this complexity of merging differing application, then further research is needed to ensure seamless updates and synchronization of disparate systems so as to avoid duplication and erroneous correction of entries due to differing time stamps.

A hospital-based EPR, enables the Primary care to see records through a portal. However, for the patient who is mobile, and moves out of their local catchment area, then their health records, currently, do not follow them easily. So, information may be lost to third parties beyond the reach of the hospital-based EPR. Truly mobile methods to enable the patient to see their records and to access their data are of high priority. The development of the NHS application by NHS digital is a means to address that.

Third-party organizations, such as *The Patient Knows Best* [25] and Clevermed [26], have developed a Web-based system whereby patient details are located in central servers, but access is via a web-based application and can enable notes to be accessed anywhere. The NHS currently purchase these systems on an ad-hoc basis: it is not uniformly rolled out.

Maternity and Oncology services currently have patient-held paper records, but some records are also migrating to web-based – the maternity system is one such migration. Again, this strategy is part of the NHS ethos, but currently not there yet: this is due to the NHS's reliance on third parties to develop the software for the NHS to use.

4.2.5 User awareness

A significant barrier to adopt and exploit advanced technologies to address security and privacy challenges in healthcare environments is the lack of user awareness. HEIR will perform several

activities in order to ensure pan-European awareness maximization towards security, privacy, and governance across all processes and levels.

First of all, standards play an important role in improving approaches to information/data security across different geographical regions and communities and also promote the successful acceptance of best practices in cybersecurity /privacy and personal data protection. HEIR will work together with relevant standardization bodies through its Advisory Board links and existing memberships of the consortium (e.g., FORTH, IMT, ITML, IBM). Moreover, HEIR will work towards forming solid links between CERTS all over the EU, exploiting FORTH's current collaborations. HEIR's goal is to extend state of the art to a set of new standards that will upgrade medical IT applications' security to a satisfactory level. The identified set of standardization bodies and EU directives that will be closely monitored during the project lifetime, meanwhile contributing towards the practical implementation of relevant EU legislation, include:

The NIS Directive: the EU directive aims to create and strengthen a *Computer Security Incident Response Team (CSIRT)* to promote cooperation between all Member States (MS) and create a culture of security across sectors such as digital infrastructure, manufacturing, transport, energy, healthcare, financial market, water. HEIR aims to contribute to the development of the solid CSIRT Network with its technological tools and modules that can be used to raise levels of the overall security and resilience in the health sector across the EU. This will be supported by the fact that the HEIR framework is targeted to SMEs/enterprises/organizations in multiple sectors, while produced white papers on behalf of the HEIR consortium and information sharing can provide valuable information regarding the evolution of this directive.

The European Union Agency for Cybersecurity (ENISA): ENISA is a center of cybersecurity expertise in Europe and supports MS for more than ten years in implementing relevant EU legislation. HEIR aims to develop advanced technologies to achieve a higher maturity level of security incident detection and mitigation, which aligns with the aim of ENISA. HEIR is planning to closely collaborate with ENISA towards a common European privacy and cybersecurity standards framework. In addition, the consortium commits to share their results with ENISA and obtain knowledge through ENISA representatives.

The EU Cyber Security Strategy: this strategy provides a harmonized framework for the evolution of three different cybersecurity aspects, which until recently had been evolving independently. Towards this direction, the HEIR cybersecurity platform can be appropriately disseminated and standardized to be widely used along with the delivered benchmarking tool.

The EU Cloud Strategy: the European Commission (EC) published its cloud strategy, entitled 'Unleashing the Potential of Cloud Computing in Europe.' Given that the ***HEIR*** framework is targeted to any health-related institutions/enterprises/organizations/centers, adherence with this strategy will be supported, while produced white papers on behalf of the HEIR consortium can provide valuable information about the evolution of such strategies.

ETSI Cyber Security Technical Committee (TC CYBER): is recognized in the EU & worldwide as trusted experts offering market-driven cybersecurity standardization solutions and guidance. TC CYBER is working closely with relevant stakeholders to develop appropriate standards to increase privacy and security for organizations and citizens across Europe. HEIR mechanisms are going to be disseminated to TC CYBER.

CEN-CENELEC-ETSI 'Cyber Security Coordination Group' (CSCG): The group aims to provide strategic advice in the field of IT security, *Network and Information Security (NIS)*, and cybersecurity. Contribution from HEIR can be used towards the preparation of a set of advice.

HIMSS Europe that is a leading health IT knowledge organization that acts as a barometer for the industry and provides valuable insights into market trends and gap analysis at a local, national and international level. HEIR strategies are going to be disseminated to **HIMSS Europe**.

NIST Cybersecurity Framework and ICS-CERT medical cybersecurity advisories*:* HEIR will collect and share information about medical objects' vulnerabilities and the appropriate mitigation actions.

Based on the aforementioned standardization bodies, the targeted standards within the HEIR consortium include:

Information Security Standards: *ISO/IEC 27001:2013* Information security management systems (ISMS), *ISO/IEC 27003:2010* Information security management system implementation guidance; *ISO/IEC 27005* Information technology — Security techniques — Information security risk management; *ISO/IEC 27014:2013* governance of information security; *ISO/IEC TR 27016:2014* Information security management - Organizational economics, *ISO/IEC 27039:2015* Selection, deployment and operations of intrusion detection systems (IDPS), *ISO/IEC 27040:2015* Storage security, *ETSI TR-103-305* Critical Security Controls for Effective Cyber Defense;

Data Protection and Privacy Standards: *ISO/IEC 27018:2014* Code of practice to protect personally identifiable information (PII) in public clouds acting as PII processors, *ISO/IEC 29100:2011* Privacy framework, *ISO/IEC 29101:2013* Privacy architecture framework, *BSI BS 10012:2009* Data protection. Specification for a personal information management system, *CEN CWA 16113:2010* Personal Data Protection Good Practices

Third Party Security Management Standards: *ISO/IEC 27036-1, 2 and 3:2014* Information security for supplier relationships - Parts 1, 2 and 3, *ISO 28000:2007* Specification for security management systems for the supply chain

Apart from the standardization activities, HEIR will focus on raising cybersecurity awareness to executives and employees in the healthcare sector, defining the duties, responsibilities, and communication procedures and protocols of all the members, ensuring at the same time alignment with current directives and legislations; thus, significantly advancing Security Governance in the health sector.

Moreover, HEIR will set up a broad European network for establishing good security practices in all regulatory frameworks to reduce market access. The HEIR Observatory for the Security of Electronic Medical Devices (OSEMD) will be a cybersecurity and resilience benchmarking tool for medical IT devices, networks, and computer services; it will act as a public repository for best practices and solutions towards healthcare cybersecurity as well as a monitoring service for cybersecurity issues in the medical sector. This will enable healthcare stakeholders to safely access, monitor, and share information about HEIR good practices/successful scenarios and mitigate the identified challenges, problems, and vulnerabilities. Based on the data collected, HEIR aims to compile a list of the Top 10 programming errors and systems misconfigurations in medical software. The Top 10 Threats for Medical Systems will serve the software industry as a checklist of issues that should be addressed when developing medical applications or software for medical devices. It will ensure that the developers are aware of the most serious risks and take the appropriate measures to mitigate them. More than that, analytical guidelines and recommendations will be prepared and presented to enable the EU to start a fruitful discussion on the necessary directives that should be introduced to be applicable to software being developed for medical systems. At this point, the security of electronic devices and applications in the healthcare ecosystem is more an organizational and procedural challenge

rather than a technical one. The HEIR Observatory will highlight these shortcomings and will promote viable, secure alternatives.

To complement all the above activities, HEIR will focus on building a large community and an ecosystem around the project's results and impact assessment outcomes that will promote public awareness for security and privacy in the healthcare domain. This community will be nurtured through networking and liaisons with technical and domain-specific communities, policymakers and local authorities, EU associations (i.e., EuroVR, BDVA), other EU projects, and more.

4.2.6 Trust increase

The Health Care Industry Cybersecurity Task Force report [27] also provides two imperatives to Develop the health care workforce capacity necessary to *prioritize and ensure cybersecurity awareness and technical capabilities* (*Imperative 3*) and to *increase health care industry readiness through improved cybersecurity awareness and education* (*Imperative 4*). It is universally recognized that undertrained employees are organizations' biggest cybersecurity weakness. The problem is even more evident in healthcare since the operator's attention is attracted to her/his main priority, the patient's health. According to a study issued by the Ponemon Institute in 2016 [28], 36% of healthcare organizations that have been breached point to unintentional actions by their employees as the cause. In November 2016 alone, 54% of breaches were caused by employee error, a record month for breaches. So, similarly to proper hospital hygiene practices, cybersecurity cannot become a common practice without training and education. For example, a recent survey [29], addressed to qualified employees of providers and payers in the United States and Canada, reports that 21% of healthcare employees write down username and password near the computer. An effective training model should teach them to avoid this behaviour.

There is broad evidence [30] [31] that security awareness training is the most cost-effective form of security control. On the other hand, a meaningful approach to the training cannot be based only on the transmission of technical and legislative information and you have to consider which is the perception of the risk as seen from a psychological point of view [32] [33]. The problem has been around for some time and, currently, there are a lot of training courses available in the market. Most of them are supplied online [34]. Some of them stimulate interactivity, a fundamental element for the training's success [35]. However, they are often focused on specific threats, like phishing, with marginal care on other aspects, which are equally important, especially in the healthcare environment. Because of the subject's practical relevance, organizations such as SANS are involved in the definition of training programs and certifications, taking into account the specific area of healthcare professionals. However, the major part of the training programs takes as a reference point, the US scenario, where the legislative and organizational framework is often different from Europe.

Key points in the training are the awareness and human behaviour of people involved, mainly focusing on cybersecurity assurance. In the healthcare sector, continuing education and professional development are crucial to maintain and advance skills and knowledge in an environment that is continuously changing due to new healthcare research and technology. E-learning provides a solution to these challenges, allowing healthcare professionals to follow the training at their own pace at a time and location that suit them. Sometimes online training does not suffice, though (e.g., when lab training is necessary), in which case a hybrid solution (known as blended learning), where part of the course is delivered through classroom lectures, can exploit the best of both worlds. The ability to include interactive and multimedia elements in e-learning is also vital because it can help improve retention and understanding of medical course material that is often very visual. Indeed, the result of a study conducted on these issues

[36] indicated that different delivery models should be used together to get the maximum benefits out of the information security awareness program.

Another appealing opportunity is found in using gamification. By this term, we mean “the use of game design elements in non-game contexts”. Gamification is often employed in health and wellness apps related to self-management, disease prevention, medication adherence, medical education-related simulations, and some telehealth programs [37] [38] [39].

5. State of the art

This section provides a comprehensive analysis of the state-of-the-art, updated with respect to the HEIR proposal, highlighting the projected advances of HEIR, both for the HEIR platform as a whole and for each specific scientific and technological domain of interest to HEIR. In addition, an internal survey (see Appendix) assisted the more targeted focus of this section.

5.1 Security and privacy assessment

Healthcare environments such as hospitals are increasingly relying on connected devices, large and small. Such environments' complexity makes risk management extremely difficult, given the large attack surface [40] [41]. Therefore, cyber-risk assessment is becoming a critical part of running a hospital's IT network, as indicated in the report from the Health Care Industry Cybersecurity Task Force [27]. This report's first imperative cites this methodological aspect as the top priority for cybersecurity in healthcare. The establishment of such a reference cybersecurity framework and methodology for healthcare is specifically mentioned as a recommendation of the report, as well as the establishment of scalable best practices for governance.

While there are several general-purpose cybersecurity methodologies available, the most well-known being the Cybersecurity Framework proposed by the *National Institute of Standards and Technology (NIST)* [42], there is no such document that helps to manage the many peculiar and often conflicting requirements of the healthcare environments. Work carried out in HEIR related to the RAMA score, and the observatory is particularly relevant to support up to date and quantified cybersecurity and privacy risk assessment.

5.2 Security and privacy preservation

One of the foremost issues of medical environments is the protection of data, be it medical or administrative, in an environment where expressing security policies is difficult. The medical world is increasingly relying on its data for diagnosis and treatment, therefore on sensors and devices to create this data and communications channels to collect, store, and exchange it. Medical activity is likely to become mostly analytics-driven, taking advantage of the volume of data collected by large and small devices. This creates both new opportunities and new threats. The Health Care Industry Cybersecurity Task Force report [27] provides the need for protection of data is further reinforced by the entry into law of the GDPR [43].

HEIR will rely on standards, specifically Health Level 7 (HL7), to enhance its solutions' applicability. The most prevalent system for describing EPR is the Health Level Seven (HL7) *Clinical Document Architecture (CDA)* [44] [45].

Another critical aspect is the sharing of data through cloud computing and storage solutions. The latter has become very common among enterprises in general and among hospitals and healthcare facilities in particular. One of the main benefits is the simplification of the information sharing process among multiple organizations or departments, which is a fundamental requirement in the healthcare world: the patients meet many practitioners (doctors, nurses, etc.) and organizations (hospitals, laboratories, nursing homes, etc.) over a long period of time: efficient and secure information sharing strategies among these stakeholders can have a huge impact when the lives of patients are on the line. However, storing sensitive health records in the cloud, whilst enabling increased availability, exposes the security and the privacy of these records to the risk of being violated [46] [47]. Recent developments in cloud architectures have originated new models of online storage clouds based on data dispersal algorithms [48] [49] [50]. Existing solutions have been explicitly applied in the healthcare world to address the well-known issues of privacy and confidentiality that arise when patients'

data are transferred to remote cloud storage services [51] [52] [53] [54] [55]. Ensuring confidentiality in this context is crucial: only legitimate users should access any part of the information they distribute among storage nodes. The key idea behind all such solutions is that the data is divided into several distributed pieces among remote and independent storage nodes. Formal analysis techniques have been employed to assess their degree of confidentiality against honest-but curious cloud storage providers and external attackers [56].

5.3 Electronic medical devices security and trust

Electronic medical devices (EMDs) offer a plethora of possibilities in the healthcare domain, aiming to increase the ability of healthcare providers to treat patients and improve healthcare overall. They provide services for better patient monitoring, early and more precise diagnosis, online medical treatment, disease prevention, automated control, and central reporting and monitoring of data. These services involve access to personal medical data. These services can also be offered across borders, giving citizens the feeling of security in this respect.

However, in order for all stakeholders to fully benefit from and trust electronic medical devices, they must be appropriately designed, implemented cost-effectively, and provide an acceptable level of security and privacy. The cybersecurity of medical devices is a complex and challenging ecosystem, which gradually has become a major concern to healthcare organizations, device manufacturers, and patients (Figure 6).

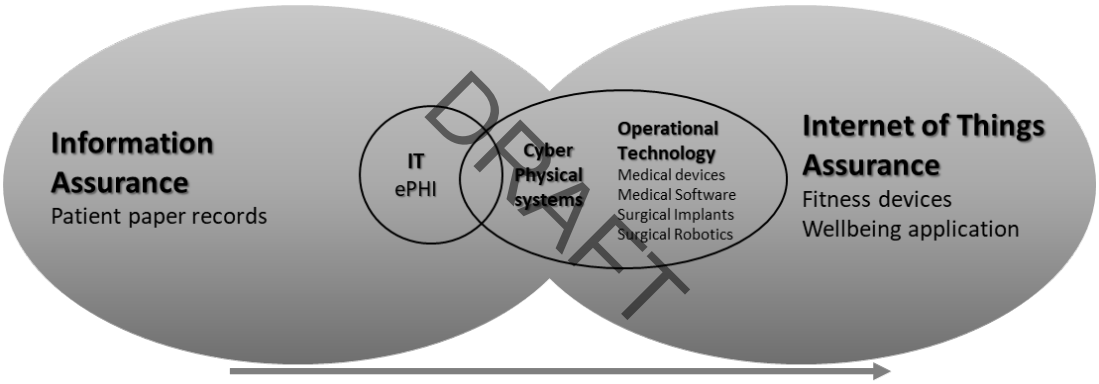

Figure 6: The healthcare cybersecurity landscape is changing rapidly

EMDs are increasingly connected to the Internet, hospital networks, and other medical or smart devices to provide their features, which increases the risk of potential cybersecurity threats. The computer technology and software, as well as the convergence of networking, has allowed the integration of healthcare systems with Information Technology (IT) through remote accessibility, facilitating the revolution of cloud-based services, and the usage of "big" data analytics. Medical devices currently integrated with an increasingly digital healthcare infrastructure are vulnerable to the same security threats, as any other IT component [57], potentially impacting the safety and effectiveness of the device. Threats and vulnerabilities cannot be eliminated; therefore, reducing cybersecurity risks is especially challenging.

Over the years, commercial medical solutions have complied with the minimal *Food and Drug Administration (FDA)* regulations on the medical devices and their data and have included secure communications. However, due to the long lifecycle of such devices, updating the equipment to purchase new hardware components or even performing software updates is not easy. The security of medical devices is an aspect that must be separately addressed in all involved technologies i.e., the medical devices themselves or other devices that are used, the different networks-wireless connections, and the healthcare delivery platforms [58], [59]. This can be further complicated, if additional connected devices such as smart phones and tablets provide the healthcare service (Figure 7).

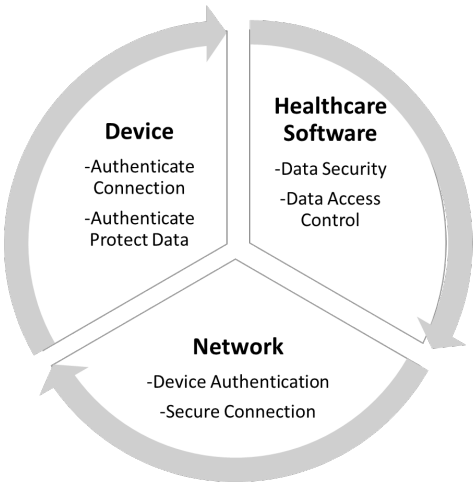

Figure 7: The security of medical devices

Based on an ENISA study from 2016 [60], we can identify four principles for secure products, services and processes:

- Security by design – the product, service or process has been conceived, designed and implemented to ensure the key security properties are maintained: availability, confidentiality, integrity and accountability;
- Security by default – the product, service or process is supplied with the confirmed capability to support these security properties at installation;
- Security throughout the lifecycle – security should be maintained from initial deployment through maintenance to decommissioning;
- Verifiable security – each of the above principles should be verifiable.

Based on these principles, the main cybersecurity and privacy research challenges related to HEIR are described below. Key points to be considered in wireless medical devices is the fact that security and cryptography functions must have very small power consumption fingerprint, key agreement and authentication, authorization must be done without patient involvement and information must not leak from the device through some side channel.

5.3.1 Interoperable and scalable security management in heterogeneous ecosystems

The definition of security management policies to deal with heterogeneity and interoperability across domains, systems and networks, introduces several challenges related to the employed security models, the language and the level of abstraction required to govern the systems. This issue is exacerbated in healthcare deployments which are comprised of heterogenous disparate data sources and networks protocols/systems. Article 20(1) of the GDPR states that a data subject has the right to "receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format", and the right to "transmit those data to another controller". The GDPR article implies the need to have interoperability between different information systems. Popular international standards for interoperability are openEHR24/05/2019 21:54:00 [61], HL7 [62] and HL7 FHIR [63].

Medical devices (i.e., ECG recorder, blood pressure recorder, clinical laboratory systems for blood samples, etc.) generate different data and need to interoperate with the electronic health record implemented in the healthcare organization. Therefore, structural and semantic interoperability is an inherent part of the data generation. In addition, foundational interoperability lets the data transmitted by one healthcare information system to be received by another.

5.3.2 Reliable and privacy-preserving identity management and user authentication

Identity management systems require new security and privacy mechanisms that can holistically manage user's/object's privacy, ID-proofing techniques based on multiple biometrics, strong authentication, usage of breeder documents (e.g., eID, ePassports), while ensuring privacy-by-default, unlikability, anonymity, federation support, non-reputation and self-sovereign identification management. The challenge is to manage properly all these features for mobile, online or physical/face-to-face scenarios, while maintaining usability and compliance with regulation e.g., GDPR [64] and eIDAS [65]. This will ultimately lead to reduction in identity-theft and related cybercrimes.

Key generation and key agreement in *Body Area Network (BAN)* for wireless medical devices have been proposed that relies on using biometrics, or physiological values (PVs) [66] like *Electrocardiograms (ECGs)* [67] which relies on time interval between heartbeats, or interpulse interval (IPI) randomness.

Biometrics are nowadays a popular form of user authentication due to their ease of use, robustness and uniqueness compared to traditional knowledge-based systems, such as PINs and passwords. This has been seen especially on smartphones, where the use of fingerprints and face authentication to unlock the device is becoming more prevalent. Moreover, the wide availability of mobile sensors allows for the deployment of near frictionless multi-modal user authentication systems.

Behavioral biometrics [68] are a particular kind of authentication factor that verifies the identity of users by the way they behave. They operate in the background in a continuous manner while the user interacts with an application. Typical examples of behavioral biometrics are keyboard dynamics [69] and mouse movements [70], and voice biometrics [71]. Sensor based gait recognition is also explored as a solution for unobtrusive user authentication [72], [73], [74], [75] with a wide applicability in wearable devices [76], [77]. By enabling continuous user authentication, gait authentication is a natural candidate for multi-modal settings, i.e., combining different types of biometric authentication factors. In this way, we can not only improve the accuracy of the user authentication system, but also strengthen the system against forging and spoofing attacks, while offering a user-friendly experience.

However, as soft biometrics like age, gender or race are linked to physiological or behavioral traits of the user, misuse of biometric templates may lead to severe privacy leakages for the user [78]. Previous work [79], [80] [81] has already shown the presence of sensitive data in biometric traces, including medical conditions and soft biometrics. In the case of gait-based user authentication, Garofalo et al. [82] demonstrated the feasibility of age and gender estimation from gait traces in the frame of the OU-ISIR Wearable Sensor-based Gait Challenge: *Age and Gender (GAG)* competition. To overcome these challenges, researchers have developed schemes which can detect the wearer of a wearable device through their physiological signals [83], [66] like ECGs [67], [84], relying on time between heartbeats, or *Interpulse Interval (IPI)* randomness, or bioelectrical impedance signals [85].

Privacy as Control can be implemented through *Privacy Enhancing Technologies (PET)*, ensuring selective and minimal disclosure of credentials and personal attributes, e.g., Anonymous Credential Systems [86], such as Idemix [87], which employs *Zero Knowledge Proofs (ZKPs)* reveal the minimal amount of information to the verifier (usually a service provider), even without disclosing the attribute value itself. However, current Anonymous Credential Systems implementations such as Idemix are complex and difficult to manage by final users.

Identity Management based on *Self-Sovereign Identities (SSI)* systems [88] focus on providing a privacy- respectful solution, enabling users with full control and management of their personal identity data without needing a third-party authority taking over the identity management operations. Thus, citizens are not anymore data subjects; instead, they become the data controller of their own identity as they can determine the purposes and ways in which personal data is processed, as they manage directly their personal data during their online transactions.

5.3.3 Powerful user authorization and access control

In all security initiatives, ensuring who gets access to what in a legal, controllable, proportional and auditable manner is key. Limiting access to resources by establishing permission rules provides for better control over users' actions. Authorisation should be granted on the principle of least privilege, granting no more privilege than is required to perform a task/job, and the privilege should not extend beyond the minimum time required to complete the task. This restrictive process limits access, creates a separation of duties and increases accountability. *Privileged Access Management (PAM)* should be a tool used to control who accesses data and the systems being accessed.

While the cookie-based authorisation is used as the de-facto standard for communication between client server applications, this technology cannot be used when we have a multi-domain networks, taking this into account a new token-based technology (RFC7519) [89] was proposed that allows to make AJAX/REST calls to other domains, by including the user information in HTTP header of the http request. This authorisation mechanism cannot cope with the heterogeneity and diversity of health and care specific IoT devices and applications.

Enrolment over Secure Transport (EST) [90] is a protocol for bootstrapping certificate and the associated *Certification Authority (CA)* certificates over TLS and HTTP. The *IETF Autonomic Networking Integrated Model and Approach (ANIMA)* working group uses EST for a solution for automated *Bootstrapping Remote Secure Key Infrastructures (BRSKI)* [91], using certificates that are conceived for large scale, but it is not considered for constrained devices.

The OAuth is a delegated authorization framework enabling secure authorization for applications on top of the transport layer i.e., http-over-TLS. It allows the client-server applications to communicate and exchange data in a way to prevent eavesdropping and tampering [92]. Several works have been done regarding the OAuth security and its application in constrained environments. The scheme [93] focuses on using OAuth to allow only authenticated users to access the IOT network. Tysowski [94] discusses use of OAuth 2.0 for secure authorization of services running on different platforms. It discusses how OAuth can be combined with Open ID to provide both authentication and authorization. Solapurkar [95] proposes a scheme based on OAuth 2.0 and JSON Web Token [96] for securing existing health care services in the IOT cloud platform.

Alternatively, access control and authentication in BAN enabled devices has been proposed to be done using distance bounding protocols [97], [98] including anomaly detections in the wireless channel [99]. However, distance bounding by itself provides for only weak authentication and can be compromised by various attack techniques [100] (like the replay attack of Kfir et al. [101]). Further, authentication can be also done using out-of-band channels like audio or visual channel signals outside the standard communication channel [102].

5.3.4 Efficient and secure cryptographic mechanisms for data sharing and analysis

Healthcare organizations collect both administrative and clinical data relevant to support and improve the wellness, health and healthcare of individuals. The importance of these data depends on the users who have authored them. Article 32 of the GDPR states the encryption of personal data as a way of ensuring data security.

End-to-end encryption of shared data, in transit and in rest, while maintaining usability and efficiency on the end-user side is an open research challenge that still needs to be covered effectively to protect user's privacy. In this sense, new techniques, algorithms and protocols, e.g., those based on proxy re-encryption, are needed to reinforce security/privacy while outsourcing the computation to Cloud wallets to minimize user's risks in protecting crypto-material. In addition, new crypto-privacy techniques are needed to guarantee authenticity on the data through novel signatures schemes. Securing a medical device from software and hardware attacks is a demanding problem due to its small processing power and low power consumption requirement (BAN based devices) or its proprietary software.

One of the most popular cryptographic mechanisms involves the use of *Attribute-Based Encryption (ABE),* which utilises a public key cryptography to eliminate unauthorised data access in the cloud [103]. ABE encryption is employed in a number of eHealth system architectures [104], [105], [106], [107], [108]. Other mechanisms are the *Identity-Based Encryption (IBE)* [109], which places emphasis on the encryption of the data source and *Homomorphic Encryption (HE)* [110], which allows calculations to be performed on encrypted data without decrypting it first.

However, cryptographic schemes (especially public key cryptography) used in security apps are computationally and memory demanding. Lightweight cryptography schemes can be used to solve this [111] but however do not offer very strong security. Non lightweight solutions, such as EST over secure CoAP [112] propose an adaptation of EST for constrained devices, i.e., IoT devices, that work on top of *Datagram Transport Layer Security (DTLS)*. This has the consequent limitations that some devices will lack the resources to handle large payloads managed in EST-coaps.

On another note, all exchanged data should be encrypted, without intermediate entities such as proxies or cloud-providers being able to access the user's data. Data minimization and privacy-by-default properties, above all, in emerging distributed deployments needs to be guaranteed. Thus, novel cryptoprivacy protocols, mechanism and systems, such as those based on Zero-knowledge proofs, are needed to ensure anonymity, minimal disclosure of personal information, above all in public Clouds, ledgers and mobiles, while ensuring the user's rights laid out in GDPR.

Health data analytics, one of the EMD provided services, raises new concerns about privacy preservation, as the possible dynamic combination of large data coming from diverse sources can undermine anonymity, pseudonymity properties that can be given for granted in a single domain. The MapReduce framework is one of the best approaches used by industry leaders to implement cryptographic security in large datasets [113]. Currently, HE is also being exploited for health data analytics to perform computations on encrypted data without compromising patient privacy [114].

5.3.5 Deter unethical use of health information via audit trails

Audit trails, or records of information access events, can provide one of the strongest deterrents to abuse. Audit trails record details about information access, including the identity of the requester, the date and time of the request, the source and destination of the request, a descriptor of the information retrieved, and perhaps a reason for the access. The effectiveness of such a record depends on strong authentication of users having access to the system. Audit trail information must also be kept in a safe place so that intruders cannot modify the trail to erase evidence of their access. Finally, although there is some benefit in users' *thinking* that an audit trail is being kept and analyzed, such trails are truly effective only if their information is *actually* reviewed and analyzed.

Effective software tools are needed to maintain continuous surveillance of audit trail information so that abuses are detected quickly and sanctions meted out, both to maintain the effectiveness of audit trails as prevention tools and to contain, as soon as possible, the extent of any abuse. Blockchain [115] is the best-known distributed ledger technology; a ledger is a database which keeps a final and definitive record of transactions. Records, once stored, are immutable and cannot be tampered without leaving behind a clear track. Blockchain enables a ledger to be held in a network across a series of nodes, which avoids one centralised location and the need for intermediaries' services. This is particularly helpful for providing trust, traceability and security in systems that exchange data or assets. Blockchains have found applicability in sectors ranging from banking and finance to public services and healthcare [116].

Gipp et al. [117] presented a decentralized trusted timestamping system. It enables users to prove that they were in possession of a file at a specific point in time in the past. Users have to hash the file and embed the produced hash value in a bitcoin transaction. The integrity of the data is ensured by the blockchain; checking the public ledger of transactions to check the validity of the proof of possession is trivial. Dot-bit [118] is a decentralized domain-name registration service that practically runs on Namecoin [119], one of the first forks of bitcoin. Dot-bit replaces domain-name controllers by a public ledger that moves domain-name registration records from the servers to the clients. Controllers as single points of failure are eliminated, while many web attacks targeting DNS servers become irrelevant. The authors in [120] implement a decentralized *Public Key Infrastructure (PKI)* service. Their system, called Certcoin, has no central authority, and requires the use of secure distributed dictionary data structures in order to store data related to the keys. Certcoin is implemented on bitcoin infrastructure. Recently, the connection of the IoT to blockchain has drown significant attention, mainly because of a relevant joint research between IBM and Samsung [121]. ADEPT is a system that uses elements of bitcoin's underlying design to build a distributed network of devices, – a decentralized Internet of Things. It taps blockchains to provide the backbone of the system, utilizing a mix of proof-of-work and proof-of-stake in order to secure transactions. IBM and Samsung chose three protocols – BitTorrent (file sharing), Ethereum (smart contracts) and TeleHash (peer-to-peer messaging) – to underpin the ADEPT concept. In [122], a peer-to-peer secure communication system is described for the IoT. The authors try to limit the required computational and communication effort for the nodes, while keeping the security requirements satisfied. However, even though they protect the communication, the storage of information remains unprotected. The protocol presented mainly decentralizes storage, in order to diminish the negative effects of centralized storage schemes. Another relevant approach is presented in [123], wherein a heterogeneous network infrastructure is designed, to allow different applications in the IoT to interact with sensors and actuators.

5.3.6 Encryption of communications

Each type of external access to health care information resources poses possible security vulnerabilities that could compromise patient privacy. One area where recent advances has been made to improve the security (and arguably also privacy) of users is in the encryption of communications. Some recent advances have made such *End-to-End Encrypted (E2EE)* messaging a commonplace and easy to use experience for hundreds of millions or even billions of users.

The important technology behind this development is the Signal protocol by Open Whisper Systems [124] and the Signal application [125]. When WhatsApp adopted this technology to provide E2EE messaging for their users, it signaled a major change in the encryption landscape of communications between individuals. Of course, there are many other applications that now provide similar protection of communications and even Facebook is said to be contemplating

adding E2EE messaging to their Messenger application [126]. Several examples [127] show, that it is possible to achieve great security benefits through secure messaging, without affecting user experience in any meaningful way.

E2EE is not the only field where additional security can be achieved through encryption. Network traffic has been largely unencrypted until some recent developments that have produced website developers' easy tools to make their sites run HTTPS, the encrypted version of HTTP. The Let's Encrypt -project provides an easy way to secure your website and their statistics show a remarkable increase in HTTPS adoption [128]. HTTPS has been available for a long time, but the setting up of a certificate and all other setup for the encryption has been hard for the administrators.

For the end users, many browsers offering functionality that will enforce HTTPS is used in browsing whenever possible [129]. This makes the user experience very smooth also for the web end users. Of course, this type of encryption brings some side effects such as that users tend to ignore security warnings (e.g., because a certificate has expired) and thus can be exposed to phishing etc. [130]

To further protect wireless medical devices, external modules mediating communication with the Medical device and providing both confidentiality for transmitted data and protection against unauthenticated communication, have been proposed. Such devices are the cloaker [131], the IMDGuard [132] or use friendly jamming tokens as the ones in [133].

5.3.7 Compliance to legal and regulatory frameworks and standards

Legal and regulatory developments related to cybersecurity are increasing in the last decades. At European level, GDPR (General Data Protection Regulation) [64] and ISO 27001 [134] are two important compliance standards that aim to strengthen data security and reduce the risk of data breaches. GDPR is a regulation in EU law that regulates how companies process and protect personal data relating to individual citizens in the EU. ISO 27001 is an international management standard that provides a proven framework for managing information security. It uses an integrated set of recommended policies, procedures, documents and technologies in the form of an Information Security Management System.

Patient safety risks related with medical devices or software, are typically managed through specific frameworks which focus on the device/software to be developed. For example, ISO 14971 [135] provides a Risk Management Framework designed for the development of medical devices. Furthermore, ISO/TR 27809:2007 [136] provides guidance regarding patient safety in the context of the ISO 27000 family of standards related with software security. More specifically, ISO TR 27809 identifies specific controls which can be used as guide to identify and manage possible Patient Safety risks related with the Medical Software security issues. Moreover, European Commission provides a regulation framework regarding Medical Device development consisting of several directives regarding application of security measures, the application of CE marking etc. [137]. Respectively, FDA provides guidelines on post market management of Cybersecurity in Medical Devices [138], also focusing on preventing patient harm. The above regulation and technical risk management frameworks and standards, are characterised by the following features:

a) They focus on the industry perspective and tend to provide guidance on how to manage risks from a manufacturer point of view and do not actively engage healthcare professionals who are the main people responsible for the overall Patient's Safety;
b) They do not emphasize on the healthcare setting context which is volatile and subjective (e.g., prioritisation of needs and risk-benefit relationships is heavily dependent on specific patient and healthcare process);

c) They define rigorous and hard to adopt risk management approaches which typically refer to cybersecurity experts and therefore are not easy to apply in a flexible manner in a real-world healthcare context.

5.3.8 Related EU projects

Table 1 summarizes the main related research projects, and their relationship with HEIR in terms of the EMD security and trust. The HEIR consortium will create synergies with them, aiming at reuse of 'know-how' in order to improve HEIR offering.

Table 1: Related research projects

Project Name	Description	Keywords related to EMD security and trust
ASCLEPIOS	The vision of ASCLEPIOS (https://www.asclepios-project.eu/) is to maximize and fortify the trust of users on cloud-based healthcare services by developing mechanisms for protecting both corporate and personal sensitive data. While researchers have developed many theoretical models that could enhance the security level of healthcare services, only a rudimentary set of techniques are currently in use. ASCLEPIOS is exploiting this gap by using several modern cryptographic approaches to build a cloud-based eHealth framework that protects users' privacy and prevents both internal and external attacks.	Secure data sharing; Authorisation
MyHealthMyData	MyHealthMyData (MHMD http://www.myhealthmydata.eu/) aims at fundamentally changing the way sensitive data are shared. MHMD is poised to be the first open biomedical information network centred on the connection between organisations and individuals, encouraging hospitals to start making anonymised data available for open research, while prompting citizens to become the ultimate owners and controllers of their health data. MHMD is intended to become a true information marketplace, based on new mechanisms of trust and direct, value-based relationships between EU citizens, hospitals, research centres and businesses.	Secure data sharing; Traceability and auditability
PANACEA	PANACEA (https://panacearesearch.eu/) is driving a people-centric approach to cyber security in healthcare. Running from January 2019 to December 2021, this research and innovation action will design, develop and deploy the PANACEA Toolkit for uptake in hospitals, care centres and other medical facilities.	Identification & authentication; Secure data sharing; Interoperability
FeatureCloud	FeatureCloud (https://featurecloud.eu/) is a transformative, pan-European research collaboration and AI-development project which implements a software toolkit for substantially reducing cyber risks to healthcare infrastructure by employing the worldwide first "privacy by design" approach.	Secure data sharing
KONFIDO	KONFIDO is a H2020 project that aims to leverage proven tools and procedures, as well as novel approaches and cutting edge technology, in view of creating a scalable and holistic	Secure data sharing;

	paradigm for secure inner- and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way both at national and European levels.	Traceability and auditability
Serums	The Serums Project (https://www.serums-h2020.org/) deals with security and privacy of future-generation healthcare systems, putting patients at the centre of future healthcare provision, enhancing their personal care and maximising the quality of treatment they receive.	Secure data sharing; Authorisation; Network encryption; Legal compliance
SPHINX	SPHINX (https://sphinx-project.eu/) aims to introduce a Universal Cyber Security Toolkit, thus enhancing the cyber protection of Health IT Ecosystem and ensuring the patient data privacy and integrity. It will also provide an automated zero-touch device and service verification toolkit that will be easily adapted or embedded on existing, medical, clinical or health available infrastructures.	Secure data sharing
CUREX	The vision of CUREX (https://curex-project.eu) is to safeguard patient privacy and increase their trust in the currently vulnerable critical healthcare information infrastructures, especially in cases where data is exchanged among healthcare stakeholders within any business, operational and systemic cross-border environment.	Secure data sharing; Traceability and auditability
e-SENS	e-SENS (http://www.esens.eu/) focuses on cross-border interoperability in eHealth, eJustice and eProcurement, aiming to provide generic and re-usable software components for, inter alia, e-Delivery, e-Identity (eID) and e-Signature. Among other tools they provide a standalone adapter in the e-ID area to bridge the gap between e-IDAS based German middelware and the Dutch PEPS based on STORK 2.0. In addition the e-SENS project developed an 'Evidence Emitter', a mechanism for achieving non-repudiation in cross-border communication though evidence generation and collection (https://tinyurl.com/n72xgjc), and a reference architecture (https://tinyurl.com/l8dbugc)	Identification & authentication; Interoperability
SHIELD	SHiELD (https://www.project-shield.eu/) will unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges that today prevent this data being exchanged with those who need it. This will make it possible to provide better health care to mobile citizens across European borders, and facilitate legitimate commercial uses of health data.	Secure data sharing; Legal compliance
STORK 2.0	STORK 2.0 contributed to the realization of a single European electronic identification (e-ID) and authentication solution. It built on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities. The results of the STORK project are currently available via the CEF Digital Portal [139].	Identification & authentication

5.4 Healthcare systems security assurance

To provide details about the healthcare systems' security assurance, we provide a real-world case scenario. CUH and its satellite community sites have around 4.5k users. In order to utilize Croydon IT equipment, every user would need to have a CHS domain account. These users will then connect to *Health and Social Care Network* (HSCN) and the internet either via physical LAN connection or via NHS secure WIFI or when connecting from either a home or unsecured network would connect into the CHS network via VPN.

An additional layer of security exists when access to clinical systems such as Cerner, requires a valid smart card to gain access. The majority of employee-facing hardware is on the Windows 10 Operating system, and a program is currently running to migrate all remaining devices to Windows 10. For the CHS Server layer, most servers and Firewalls operating systems are either Server 2012 or 2019. For medical devices where data leaves the CUH site, most would be physically connected to the CUH LAN. The significant majority of this data is passed onto a single system, called Cerner, via a dedicated Firewall cluster.

When a third party obtains patient data on behalf of the NHS, for example, via third party heart monitors being sent to patients, the sharing of data between CHS and the third party is governed via a data-sharing agreement, and data is transferred securely via portal login with dedicated user access. In addition to the initial user login and domain account controls, CUH utilizes Palo Alto firewalls to restrict unauthorized access to external sites.

All workstations and servers within CHS have Antivirus installed to secure both servers and end-user devices. Also, all Servers and workstations utilize Microsoft ATP. Generic sign-on devices Computers on wheels (COWs), Workstations on Wheels (WOWs), and Drug Trolleys are locked down such that only the required medical tooling is accessible. Users' access to laptop or desktop settings etc., is locked down. As standard, USB ports on all user devices, including laptops, COWs, and WOWs are disabled via global policy rules and only enabled in exceptional circumstances and with exec approval. CHS is assessed against the Data Security & protection toolkit and cybersecurity essential plus. CHS' current status in this regard 'Not met' and work is progressing in order to get the Data Security and Protection toolkit signed off by NHS Digital. Cybersecurity essentials sign-off will be a follow-on activity and focus.

Currently, CUH medical devices are not fully network segregated. The desired state is to implement granular network segregation at the device type level to effectively restrict access to all but that which is essential to be functional as a device.

It is envisaged that the ***HEIR operating system would enable closer monitoring of the users on the system, such that increasing levels of activity internally, as well as increased hits on the Firewall, will enable early warning of the system under threat, enabling earlier responses to identify and isolate the threat before the system is compromised.*** Reliance on the N3 Firewall, operated by BT, may not be sufficient in the world of the evolving cybercriminal. Also, ***HEIR will add on a layer of protection not currently available: the lockdown and security of devices that may be used within the NHS Health care ecosystem.***

6. Conclusion

This deliverable presented the output of the work carried out in Task 1.1 - "The critical role of security and identity management in healthcare environments", which, as planned, was carried out in the first four months of the project (M1-M4).

The vision of HEIR is to provide a thorough threat identification and cybersecurity knowledge base system addressing both local (in the hospital/medical center) and global (including different stakeholders) levels, that comprises the following pillars: *(i)* Real-time intelligent threat hunting services, facilitated by advanced machine learning technologies, supporting the identification of the most common threats in electronic medical systems; *(ii)* Sensitive data trustworthiness sharing facilitated by the HEIR privacy-aware framework; *(iii)* 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; *(iv)* The delivery of an Observatory for the Security of Electronic Medical Devices; an intelligent knowledge base accessible by different stakeholders, providing advanced visualizations for each threat identified in RAMA and facilitating global awareness on EMD-related threats. Towards this way, this deliverable sets strong foundations upon them the whole HEIR platform can be built.

More precisely, this deliverable provides a basis for the development of the HEIR platform. Starting from the literature review, both academic and technical, a first refinement of available tools, algorithms, and methodologies was established within this deliverable. In addition, a survey took place that indicated potentially vulnerabilities in the healthcare sector. All the extracted points and knowledge will set the ground for further discussion, as they will improve and guide the progress of the HEIR platform. Additionally, the initial requirements for an effective solution will be subject to further research and improvement. Currently, they should be seen as a first proposal, which will be elaborated together with the technology partners of the HEIR project. It is necessary to precisely specify them within the project's lifetime in order to reach a common understanding of the importance and meaning of the various points we want to cover within this project.

7. References

[1] ENISA, "ENISA programming document 2019-2021," [Online]. Available: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021.

[2] Trend Micro, "The Price of Health Records: Electronic Healthcare Data In the Underground," [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/electronic-healthcare-data-in-the-underground.

[3] European Commission, "Public consultation on Transformation of Health and Care in the Digital Single Market," [Online]. Available: https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market_en.

[4] Notified, "Data Breach Resources to Help Make Better Decisions," [Online]. Available: https://notified.idtheftcenter.org/s/resource#trendAnalysisSection.

[5] World Health Organization, "WHO reports fivefold increase in cyber attacks, urges vigilance," [Online]. Available: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

[6] P. Williams and A. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Medical devices,* 2015.

[7] IBM Security, "Cost of a Data Breach Report 2020," [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

[8] Global Market Insights, "Industry Trends," [Online]. Available: https://www.gminsights.com/industry-analysis/healthcare-it-market.

[9] M. Mikulic, "Global digital health market by major segment 2015-2025," [Online]. Available: https://www.statista.com/statistics/387867/value-of-worldwide-digital-health-market-forecast-by-segment/.

[10] Allied Market Research, "Cyber Security Market Statistics - 2027," [Online]. Available: https://www.alliedmarketresearch.com/cyber-security-market.

[11] European Commission, "eHealth: Dightal health and care," [Online]. Available: https://ec.europa.eu/health/ehealth/policy/network_en.

[12] European Commission, "First EU citizens using ePrescriptions in other EU country," [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6808.

[13] European Commission, "Questions and Answers -- Commission makes it easier for citizens to access health data securely across borders," [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_853.

[14] Cloudflare, "What is OWASP? What Are The OWASP Top 10?," [Online]. Available: https://www.cloudflare.com/learning/security/threats/owasp-top-10/.

[15] ENISA, "ENISA Threat Landscape through the years," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape.

[16] Wikipedia, "Data breach," [Online]. Available: https://en.wikipedia.org/wiki/Data_breach.

[17] Wikipedia, "Medical data breach," [Online]. Available: https://en.wikipedia.org/wiki/Medical_data_breach.

[18] M. Simon and V. Looten, "Description of Data Breaches Notifications in France and Lessons Learned for the Healthcare Stakeholders," *Studies in Health Technology and Informatics,* 2020.

[19] IronNet, "IronNet Cybersecurity wins 2020 Innovative Product of the Year for Threat Detection at the Cyber Security Awards," [Online]. Available: https://www.ironnet.com/news/ironnet-cybersecurity-wins-2020-innovative-product-of-the-year-for-threat-detection-at-the-cyber-security-awards.

[20] Cyber Security Intelligence, "Machine Learning Transforms Threat Detection," [Online]. Available: https://www.cybersecurityintelligence.com/blog/machine-learning-transforms-threat-detection-5088.html.

[21] Venture Beat, "Google adds threat detection to Chronicle cybersecurity platform," [Online]. Available: https://venturebeat.com/2020/09/23/google-adds-threat-detection-to-chronicle-cybersecurity-platform/.

[22] A. G. M. Alzahrani, A. Alenezi, A. Mershed, H. Atlam, F. Mousa and G. Wills, "A Framework for Data Sharing between Healthcare Providers using Blockchain," in *International Conference on Internet of Things, Big Data and Security (IoTBDS)*, 2020.

[23] J. M. Ehrenfeld, "Wannacry, cybersecurity and health information technology: A time to act," *Journal of Medical Systems,* 2017.

[24] European Commission, "European Data Protection Supervision," [Online]. Available: https://edps.europa.eu/data-protection/data-protection/legislation_en.

[25] Patients Know Best, "Your health in your hands," [Online]. Available: https://patientsknowbest.com/.

[26] Clevermed, "Creating intelligent services and solutions to support women, newborn, and children's health," [Online]. Available: https://www.clevermed.com/.

[27] Health Care Industry Cybersecurity Task Force, "Report on improving cybersecurity in the health care industry.," 2017.

[28] Ponemon Institute, "Sixth annual benchmark study on privacy & security of healthcare data," 2016.

[29] Accenture, "Accenture 2018 Healthcare Workforce Survey on Cybersecurity," 2018. [Online]. Available: https://www.accenture.com/_acnmedia/PDF-86/Accenture-2018-Healthcare-Workforce-Survey-Cybersecurity-Transcript.pdf.

[30] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security,* 2010.

[31] S. L. Hepp, R. C. Tarraf, A. Birney and M. A. Arain, "Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system," *Health Information Management Journal,* 2018.

[32] B. Schneier, "The psychology of security," in *International conference on cryptology in Africa*, 2008.

[33] R. West, "The psychology of security," *Communications of the ACM,* 2008.

[34] Cybercrime Magazine, "Security Awareness Training For Employees, And Certification Training Programs," [Online]. Available: https://cybersecurityventures.com/cybersecurity-education/.

[35] KonwBe4, "What Constitutes Effective Security Awareness Training?," [Online]. Available: https://info.knowbe4.com/whitepaper-effective-security-awareness-training.

[36] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology,* 2014.

[37] M. Adams and M. Makramalla, "Cybersecurity skills training: an attacker-centric gamified approach," *Technology Innovation Management Review,* 2015.

[38] G. Fink, D. Best, D. Manz, V. Popovsky and B. Endicott-Popovsky, "Gamification for measuring cyber security situational awareness," in *International Conference on Augmented Cognition*, 2013.

[39] D. Johnson, S. Deterding, K.-A. Kuhn, A. Staneva, S. Stoyanov and L. Hides, "Gamification for health and wellbeing: A systematic review of the literature," *Internet interventions,* 2016.

[40] National Cybersecurity and Communications Integration Center, "Attack Surface: Healthcare and Public Health Sector," 2017.

[41] P. F. Katina, C. A. Pinto, J. M. Bradley and P. T. Hester, "Interdependency-induced risk with applications to healthcare," *International Journal of Critical Infrastructure Protection,* 2014.

[42] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity," [Online]. Available: https://www.nist.gov/cyberframework/framework.

[43] P. Voigt and A. Von dem Bussche, "The EU General Data Protection Regulation (GDPR)," *A Practical Guide,* 2017.

[44] J. S. Hooda, E. Dogdu and R. Sunderraman, "Health Level-7 compliant clinical patient records system," *ACM symposium on Applied computing,* 2004.

[45] Y. G. Jung and Y. H. Lee, "Clinical Information Interchange System using HL7-CDA," *International journal of advanced smart convergence,* 2012.

[46] B.-S. Chen, C.-Y. Hsu and J.-J. Liou, "Robust design of biological circuits: Evolutionary systems biology approach," *Journal of Biomedicine and Biotechnology,* 2011.

[47] T. Ermakova and B. Fabian, "Secret sharing for health data in multi-provider clouds," in *IEEE Conference on Business Informatics*, 2013.

[48] M. Baldi, N. Maturo, E. Montali and F. Chiaraluce, "AONT-LT: A data protection scheme for cloud and cooperative storage systems," in *International Conference on High Performance Computing & Simulation (HPCS)*, 2014.

[49] M. Li, C. Qin and P. P. Lee, "CDStore: Toward reliable, secure, and cost-efficient cloud storage via convergent dispersal," in *USENIX Annual Technical Conference (ATC)*, 2015.

[50] J. K. Resch and J. S. Plank, "AONT-RS: Blending security and performance in dispersed storage systems," in *USENIX Conference on File and Storage Technologies (FAST)*, 2011.

[51] B. Fabian, T. Ermakova and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems,* 2015.

[52] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu and K.-K. R. Choo, "Fine-grained database field search using attribute-based encryption for e-healthcare clouds," *Journal of medical systems,* 2016.

[53] L. Ibraimi, M. Asim and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," in *International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health*, 2009.

[54] K. Muthukumar and M. Nandhini, "Modified secret sharing algorithm for secured medical data sharing in cloud environment," in *International Conference on Science Technology Engineering and Management (ICONSTEM)*, 2016.

[55] M. Ulutas, G. Ulutas and V. V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *Journal of Systems and Software,* 2011.

[56] M. Baldi, E. Bartocci, F. Chiaraluce, A. Cucchiarelli, L. Senigagliesi, L. Spalazzi and F. Spegni, "A probabilistic small model theorem to assess confidentiality of dispersed cloud storage," in *International Conference on Quantitative Evaluation of Systems*, 2017.

[57] K. Stouffer, V. Pillitteri, L. S. and A. M., "NIST SP 800-82R1 Guide to Industrial Control Systems (ICS) Security," *National Insititute of Standards and Technology (NIST),* 2013.

[58] FDA, "Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication," 09 January 2017.

[59] ICS-CERT, "Hospira LifeCare PCA Infusion System Vulnerabilities (Update B)," 10 06 2012. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B. [Accessed 17 11 2020].

[60] "Indispensable baseline security requirements for the procurement of secure ICT products and services," [Online]. Available: https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-ofsecure-ict-products-and-services. [Accessed 17/11/2020].

[61] [Online]. Available: https://www.openehr.org. [Accessed 17/11/2020].

[62] [Online]. Available: https://www.hl7.org/. [Accessed 17/11/2020].

[63] [Online]. Available: http://www.hl7.org/FHIR/. [Accessed 17/11/2020].

[64] [Online]. Available: https://gdpr-info.eu/. [Accessed 17/11/2020].

[65] European Parliament, "Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," European Parliament, Brussels, 2014.

[66] K. B. Rasmussen and S. Čapkun, "Implications of radio fingerprinting on the security of sensor networks," in *3rd International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007)*, pp. 331-340, 2007.

[67] K. K. Venkatasubramanian and S. K. S. Gupta, "Security for pervasive health monitoring sensor applications," in *4th International Conference on Intelligent Sensing and Information Processing (ICISIP)*, 2006.

[68] I. Deutschmann, P. Nordstrom and L. Nilsson, "Continuous authentication using behavioral biometrics," *IT Prof,* vol. 15, no. 4, pp. 12-15, 2013.

[69] F. Bergadano, D. Gunetti and C. Picardi, "User authentication through keystroke dynamics," *ACM Trans. Inf. Syst. Secur.,* vol. 5, no. 4, pp. 367-397, 2002.

[70] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Trans. dependable Secur. Comput.,* vol. 4, no. 3, pp. 165-179, 2007.

[71] H. Feng, K. Fawaz and K. G. Shin, "Continuous authentication for voice assistants," in *23rd Annual International Conference on Mobile Computing and Networking*, pp. 343–355, 2017.

[72] C. Wan, L. Wang and V. V. Phoha, "A survey on gait recognition," *ACM Comput. Surv.,* vol. 51, no. 5, p. 89, 2018.

[73] M. De Marsico and A. Mecca, "A Survey on Gait Recognition via Wearable Sensors," *ACM Comput. Surv.,* vol. 52, no. 4, pp. 1-39, 2019.

[74] D. Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," in *Annual Norwegian computer science conference*, pp. 19–21, 2007.

[75] T. Hamme, D. Preuveneers and W. Joosen, Improving Resilience of Behaviometric Based Continuous Authentication with Multiple Accelerometers, 2017.

[76] A. Muro-de-la-Herran, B. García-Zapirain and A. Méndez-Zorrilla, " Gait analysis methods: An overview of wearable and non-wearable systems, highlighting clinical applications," *Sensors,* vol. 14, no. 2, pp. 3362-3394, 2014.

[77] S. Sprager and M. B. Juric, "Inertial sensor-based gait recognition: A review," *Sensors,* vol. 15, no. 9, pp. 22089-22127, 2015.

[78] A. Dantcheva, P. Elia and A. Ross, "What else does your biometric data reveal? A survey on soft biometrics," *IEEE Trans. Inf. Forensics Secur.,* vol. 11, no. 3, pp. 441-467, 2015.

[79] E. Mordini and H. Ashton, "The transparent body: Medical information, physical privacy and respect for body integrity," in *Second generation biometrics: the ethical, legal and social context*, Springer, 2012, p. 257–283.

[80] R. Matovu and A. Serwadda, "Your substance abuse disorder is an open secret! Gleaning sensitive personal information from templates in an EEG-based authentication system," in *IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp 1-7, 2016.

[81] American Academy of Ophthalmology, "Evidence Mounts That an Eye Scan May Detect Early Alzheimer's Disease," 2018. [Online]. Available: https://www.aao.org/newsroom/news-releases/detail/evidence-eye-scan-may-detect-early-alzheimers. [Accessed 17/11/2020].

[82] G. Garofalo, E. Argones Rúa, D. Preuveneers, W. Joosen and and others, "A Systematic Comparison of Age and Gender Prediction on IMU Sensor-Based Gait Traces," *Sensors,* vol. 19, no. 13, p. 2945, 2019.

[83] A. Burns, B. R. Greene, M. J. McGrath, T. J. O'Shea, B. Kuris, S. M. Ayer and et al, "SHIMMER—A Wireless Sensor Platform for Noninvasive Biomedical Research," *IEEE Sensors Journal,* vol. 10, no. 9, pp. 1527-1534, 2010.

[84] J. Arteaga-Falconi, H. Al Osman and A. El Saddik, "ECG Authentication for Mobile Devices," *IEEE Transactions on Instrumentation and Measurement,* vol. 65, no. 3, pp. 591-600, 2015.

[85] C. Cornelius, R. Peterson, J. Skinner, R. Halter and D. Kotz, " A wearable system that knows who wears it," in *12th annual international conference on Mobile systems, applications, and services (ACM MobiSys'14)*, New York, 2014.

[86] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 93–118, 2001.

[87] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *9th ACM conference on Computer and communications security*, pp. 21–30, 2002.

[88] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *Sovrin Found.,* vol. 29, 2016.

[89] [Online]. Available: https://datatracker.ietf.org/doc/rfc7519. [Accessed 17/11/2020].

[90] A. Clark, R. Huang and Q. Wu, "RTP Control Protocol (RTCP) Extended Report (XR) Block for Burst/Gap Discard Metric Reporting. RFC 7003 (Proposed Standard)," 2013.

[91] M. Pritikin, M. Richardson, M. H. Behringer, S. Bjarnason and K. Watsen, "Bootstrapping remote secure key infrastructures (brski)," 2018. [Online]. Available: https://tools.ietf.org/id/draft-ietf-anima-bootstrapping-keyinfra-13.html. [Accessed 17/11/2020].

[92] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol, RFC 5246, Network Working Group," 2008.

[93] E. Shamini, C. Young-Kyu, H. Dong-Yeop, K. Kang-Seok and K. Ki-Hyung, "An OAuth based Authentication Mechanism for IoT Networks," *Information and Communication Technology Convergence (ICTC),* 2015.

[94] P. Tysowski, "OAuth Standard for User Authorization of Cloud Services," in *Encyclopedia of Cloud Computing* , 2016, pp. 406-416.

[95] P. Solapurkar, "Building secure healthcare services using OAuth 2.0 and JSON web token in IOT cloud scenario," in *2nd International Conference on Contemporary Computing and Informatics (IC3I)*, 2016.

[96] [Online]. Available: https://tools.ietf.org/html/rfc7519. [Accessed 17/11/2020].

[97] D. H. Yum, J. S. Kim, S. J. Hong and P. J. Lee, "Distance Bounding Protocol for Mutual Authentication," *IEEE Transactions on Wireless Communications,* vol. 10, no. 2, pp. 592-601, 2011.

[98] D. B. Kramer, M. Baker, B. Ransford, A. Molina-Markham, Q. Stewart, K. Fu and M. R. Reynolds, "Security and privacy qualities of medical devices: An analysis of FDA postmarket surveillance," *PLoS ONE,* vol. 7, p. e40200, 2012.

[99] M. Zhang, A. Raghunathan and N. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.,* vol. 7, no. 6, pp. 871-881, 2013.

[100] A. Czeskis, K. Koscher, J. R. Smith and T. Kohno, "RFIDs and secret handshakes: Defending against ghost-andleech attacks and unauthorized reads with context-aware communications," in *15th ACM conference on Computer and Communications Security (CCS 2008)*, pp. 479-490, 2008.

[101] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard," in *1st International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM '05)*, pp. 47-58, 2005.

[102] C. C. Y. Poon, Y. T. Zhang and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.,* vol. 44, no. 4, pp. 73-81, 2006.

[103] Cloud Security Alliance, "Top Ten Big Data Security and Privacy Challenges," 2012. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Top_Ten_v1.pdf .

[104] L. Ibraimi, M. Asim and M. Petko, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," in *6th JnternationalWorkshop onWearable Micro and Nano Technologies for Personalized Health (pHealth)*, 2009.

[105] M. Li, S. Yu, K. Ren and W. Lou, "Securing Personal Health Records in Cloud Computing: Client-Centric and Fine-Grained Data Access Control in Multi-owner Settings," in *SecureComm 2010*, Heidelberg, Springer, 2010, p. 89–106.

[106] M. Li, S. Yu and Y. Zheng, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," *IEEE Transactions on Parallel and Distributed Systems,* vol. 24, no. 1, pp. 131-143, 2013.

[107] S. Narayan, M. Gagne and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in *ACM workshop on Cloud computing security workshop*, New York, 2010.

[108] A. Lounis, A. Hadjidj, A. Bouabdallah and Y. Challal, "Secure Medical Architecture on the Cloud Using Wireless Sensor Networks for Emergency Management," in *Eighth Jnternational Conference on Broadband and Wireless Computing, Communication and Applications*, 2013.

[109] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology," *Proceedings of CRYPTO 84, Lecture Notes in Computer Science,* vol. 7, pp. 47-53, 1984.

[110] [Online]. Available: https://homomorphicencryption.org/ . [Accessed 17/11/2020].

[111] S. Santiago and D. L. Arockiam, "Energy Efficiency in Internet of Things: An Overview," *International Journal of Recent Trends in Engineering & Research (IJRTER,* vol. 2, no. 6, pp. 475-482, 2016.

[112] P. V. der Stok, P. Kampanakis, S. S. Kumar, M. Richardson, M. Furuhed and S. Raza, "Est over secure coap (est-coaps)," 2018. [Online]. Available: https://tools.ietf.org/html/draft-ietf-ace-coap-est-05 . [Accessed 17/11/2020].

[113] B. Sloot, D. Broeders and E. Schrijvers, Exploring the Boundaries of Big Data, Amsterdam: Amsterdam University Press, 2016.

[114] [Online]. Available: https://patents.google.com/patent/US9819650B2/en. [Accessed 17/11/2020].

[115] M. Pilkington, "Blockchain technology: principles and applications," in *Research Handbook on Digital Transformations*, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar.

[116] [Online]. Available: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-blockchain/. [Accessed 17/11/2020].

[117] B. Gipp, N. Meuschke and A. Gernandt, "Decentralized trusted timestamping using the crypto currency bitcoin," *arXiv preprint asXIV:1502.04015,* 2015.

[118] "Dot-Bit," June 2015. [Online]. Available: https://www.namecoin.org/dot-bit/. [Accessed 17/11/2020].

[119] [Online]. Available: http://namecoin.info/. [Accessed 17/11/2020].

[120] C. Fromknecht, D. Velicanu and S. Yakoubov, "A decentralized public key infrastructure with identity retention," *Tech. rep. Cryptology ePrint Archive, Report2014/803,* 2014.

[121] V. Pureswaran, S. Panikkar, S. Nair and P. Brody, "Empowering the edge, Practical insights on a decentralized Internet of Things," IBM Institute for Business value. [Online]. Available: https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf. [Accessed 17/11/2020].

[122] H. Zhang and T. Zhang, "Short paper: A peer to peer security protocol for the inter-net of things," *Secure communication for the sensible things platform,* pp. 154-156, 2015.

[123] T. Kanter, S. Forsstrom, V. Kardeby, J. Walters, U. Jennehag and P. Osterberg, "Mediasense: an internet of things platform for scalable and decentralized context sharing and control," *ICDT2012 ,* 2012.

[124] [Online]. Available: https://open-whisper-systems.readme.io. [Accessed 17/11/2020].

[125] [Online]. Available: https://www.signal.org. [Accessed 17/11/2020].

[126] [Online]. Available: https://www.theverge.com/2019/1/25/18197222/facebook-messenger-instagram-end-to-end-encryption-feature-zuckerberg. [Accessed 17/11/2020].

[127] N. Unger and et al., "SoK: Secure Messaging," *2015 IEEE Symp. Secur. Priv.,* pp. 232–249,, 2015.

[128] [Online]. Available: https://letsencrypt.org/stats/. [Accessed 17/11/2020].

[129] [Online]. Available: https://www.eff.org/https-everywhere. [Accessed 17/11/2020].

[130] S. Egelman, L. F. Cranor and J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," in *SIGCHI Conference on Human Factors in Computing Systems*, pp. 1065–1074, 2008.

[131] T. Denning, K. Fu and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *3rd conference on Hot Topics in Security (HotSec '08)*, pp. 5:1–5:7, 2008.

[132] F. Xu, Z. Qin, C. Tan, B. Wang and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *30th IEEE International Conference on Computer Communications (INFOCOM 2011)*, pp.1862–1870, 2011.

[133] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi and K. Fu, " They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.,* vol. 41, no. 4, pp. 2-13, Aug. 2011.

[134] [Online]. Available: https://www.itgovernance.co.uk/iso27001. [Accessed 17/11/2020].

[135] [Online]. Available: https://www.iso.org/standard/38193.html . [Accessed 17/11/2020].

[136] [Online]. Available: https://www.iso.org/standard/44320.html. [Accessed 17/11/2020].

[137] [Online]. Available: https://ec.europa.eu/health/md_sector/current_directives_en. [Accessed 17/11/2020].

[138] [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. [Accessed 17/11/2020].

[139] [Online]. Available: https://joinup.ec.europa.eu/software/stork. [Accessed 17/11/2020].

8. Appendix

HEIR innovations for healthcare systems

1. Provide the name of your organization.

2. What type of data do you expect to be shared among teams and/or electronic medical devices? Select all that apply.

- ☐ Raw data coming from monitors, sensors and other medical devices
- ☐ Laboratory tests data
- ☐ Medical imaging files i.e. CT scans, digital radiology
- ☐ Reconstructed imaging from raw data i.e. ECG, EEG
- ☐ Sound signals i.e. digital stethoscopy
- ☐ Text files i.e. annotations
- ☐ Data coming from commercial wearables and fitness/health apps
- ☐ ePrescription data
- ☐ Electronic Health Records (EHR)/Patient Health Records (PHR)
- ☐ Other

If other selected in the question above, please define

3. For which purposes would you need to share data with another professional or retrieve data from a medical device? Please describe one or more possible common scenarios including information about (please add numbers to distinguish each scenario):

Challenge

Policy, legal and privacy implications

1

Main actors involved

Infrastructure/devices employed

4. Please describe all infrastructures/frameworks related to privacy and security of data that are exchanged among professionals or devices that is currently implemented in your organisation (if any).

5. Does your organization identify, profile, and monitor connected medical devices and how?

6. Are any SIEM software/product/services put in place?

2

7. In what ways do you share files and sensitive data? Which communication protocols are you using?

8. Are you GDPR compliant? Have you implemented any security framework at your organization? (in terms of: Asset management, Risk management, Identity management and access control, Awareness & training, Data security)

9. Are you aware of the NIST Cybersecurity framework (CSF) for critical infrastructure protection?

- Yes
- No

If yes, do you use it or use documents related to it?

- Yes
- No

10. Do you use cybersecurity standards published by Health agencies (e.g. US FDA, other)?

- Yes
- No

11. Do you use cybersecurity standards and best practices from other origin?

- Yes
- No

If yes, can you indicate which standards and best practices you use?

If yes, which ones?

12. Are you subject to national or EU legislations related to cybersecurity and privacy?

- Yes
- No

If yes, can you list the relevant legislations?

13. Are you receiving cybersecurity vulnerability and threat information (e.g. cyber-threat intelligence)?

- Yes
- No

If yes, which sources are you receiving from?

14. Have you suffered from cyber-attacks (e.g ransomware, etc.)?

- Yes
- No

If yes, what kind of consequence (loss of data, system unavailable for a period of time, loss of time for personnel, etc.)?

15. Are you aware of others having suffered from cyberattacks ?

- Yes

- ○ No

16. In case of a security breach:

Do you have an Incident Response Team?

- ○ Yes
- ○ No

If no, explain why.

Do you perform forensics analysis for the recovery and investigation of cyber-attacks/incidents?

- ○ Yes
- ○ No

If no, explain why.

Does your organization cooperate with external entities to correlate and share incident information to achieve a cross-organization perspective on incident awareness and more effective incident responses?

- ○ Yes
- ○ No

17. Which type of security and incident management model does your organization adopt?

- ☐ Outsource (supported by external organization)
- ☐ Inhouse (internal support)
- ☐ Other

If other selected in the question above, please define