D2.9 - Use Cases Definition and Pilot Overview Document v3

WP2 – Conceptualisation, Use Cases and System Architecture

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry		
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures		
Funding scheme	RIA - Research and Innovation action		
Start Date	1st January 2019	**Duration**	36 months
Project URL	http://sphinx-project.eu/		
EU Project Officer	Christos Maramis (HaDEA)		
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA		
Deliverable	D2.9 - Use Cases Definition and Pilot Overview Document v3		
Work Package	WP2 - Conceptualisation, Use Cases and System Architecture		
Date of Delivery	**Contractual** M30	**Actual**	M30
Nature	R - Report	**Dissemination Level**	P – Public
Lead Beneficiary	EDGENEERING		
Responsible Author	Marco Manso	**Email**	marco@edgeneering.eu
Reviewer(s):	Panagiotis Panagiotidis (KT), George Doukas (NTUA)		
Keywords	Use Cases, Application Scenarios, Pilots, KPIs		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	04/01/2021	Draft	ToC and template	Marco Manso, Bárbara Guerra, José Pires (EDGE)
0.20	11/01/2021	Draft	Content Creation	SPHINX Partners
0.30	13/04/2021	Draft	Internal Review	SPHINX Partners
0.40	31/05/2021	Draft	Review 1	George Doukas (NTUA)
0.50	01/06/2021	Draft	Review 2	Panagiotis Panagiotidis (KT)
0.60	04/06/2021	Pre-final	Update to reflect the reviewers' comments	Marco Manso, Bárbara Guerra (EDGE)
0.70	09/06/2021	Pre-final	Quality Control	Michael Kontoulis (NTUA), George Doukas (NTUA)
1.00	30/06/2021	Final	Final	Christos Ntanos (NTUA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Executive Summary

This document presents the SPHINX use cases that specifically address users' requirements and expectations on the use of new and advanced cybersecurity tools and services for the benefit of healthcare organisations and their patients. In particular, this document provides an overview and the main outcomes of the work performed by the SPHINX Consortium on the SPHINX use cases, as part of Task 2.4 – Reference Scenarios and Pilot Operations Specifications and KPIs for a period of six months (month 25 or January 2021 and month 30 or June 2021).

Based on a compound framework of critical assets, threat taxonomy and actors, attack vectors and impact, this document updates deliverable D2.9 with six new use cases (use cases 22 to 27) that enrich the set of SPHINX use cases forming a basis for the three SPHINX pilots, while assisting with the consolidation of the SPHINX user requirements and technical specifications (WP2), with the development and integration effort (WPs 3 to 6) and with the SPHINX testing and validation effort (WP7). Overall, the SPHINX use cases are intended to highlight the greatest possible breadth of the SPHINX's capabilities, whilst remaining realistic and testable in realistic conditions. They also seek, where possible, to address potential risks and limitations of the SPHINX System and its usage.

The new six use cases address relevant issues facing healthcare organisations nowadays, involving the theft of digital identities in the healthcare setting, the vulnerabilities of national healthcare data repositories, the growing adoption of telemedicine resources and how it exposes patient data, the risks associated with the transfer of patients (and their data) between healthcare organisations, the exploitation of medical equipment vulnerabilities to access patient data and the need to create additional security layers on medical devices, certifying them as secure and trusted assets in the IT ecosystem of a healthcare organisation. These new use cases enhance the basis of the SPHINX use cases, highlighting the relevant experience of the SPHINX partners, not only with respect to the awareness of the specific cybersecurity landscape of healthcare organisations but also concerning the multiple facets of SPHINX's proposed functionality and ambitioned performance.

In addition, this report discloses the relevant work SPHINX partners have been developing to support the SPHINX piloting activities, namely in what concerns the key performance indicators identified as relevant to enable the evaluation of the SPHINX's impact in cybersecurity systems and healthcare organisations. The eight key performance indicators, detailed in sub-items and their applicable success measures, are now serving as a guideline for the planning of the WP7 activities dealing with the analysis of the SPHINX pilots' outcomes and specific KPI frameworks will be detailed for each SPHINX pilot.

Overall, the key innovation attained in this document is the in-depth review of all SPHINX use cases to be well-aligned with the actual SPHINX tools' developments carried out in the project, including the addition of a set of six new use cases, representing realistically the end-users' concerns and expectations with respect to advanced cybersecurity protection for healthcare organisations and also capturing the beyond state-of-the-art capabilities of the SPHINX System. In addition, it is also innovative the work conducted for defining the right key performance indicators and success measures to be applied to the validation of the SPHINX System's performance.

Built alongside with deliverable *D2.10 - SPHINX Requirements and Guidelines v3* and the development, testing and integration work of SPHINX's technical components, the deliverable *D2.9 - Use Cases Definition and Pilot Overview Document v3* is the final result of Task 2.4 – Reference Scenarios and Pilot Operations Specifications and KPIs and reflects the prevailing project's work synergies, delivering on the predefined goal of establishing a sound foundation to support the planning and design of the three SPHINX pilots.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Acronyms

ABBREVIATION	EXPLANATION
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
API	Application Programming Interface
App	Mobile Application
BLE	Bluetooth Low Energy
BMS	Building Management System
BYOD	Bring Your Own Device
CC	Common Criteria for Information Technology Security Evaluation
C&C	Command and Control
CCTV	Closed Circuit Television
CEF	Connecting Europe Facility
CPU	Computer Processing Unit
CSRF	Cross-Site Request Forgery
CT	Computerised Tomography
DDoS	Distributed Denial of Service
DICOM	Digital Imaging and Communications in Medicine
DoS	Denial of Service
EC	European Commission
eHDSI	eHealth Digital Service Infrastructure
eHealth	Electronic Health
EHR	Electronic Health Record
ENESIS	Portuguese National Strategy for the Health Information Ecosystem
ENISA	European Union Agency for Network and Information Security
ERNs	European Reference Networks
ERP	Enterprise Resource Planning
EU	European Union
GDPR	General Data Protection Regulation
HIS	Hospital Information System
HL7	Health Level Seven
HTTP	HyperText Transfer Protocol
HTTP	HyperText Transfer Protocol with Security
HW	Hardware
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
KPIs	Key Performance Indicators

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

ABBREVIATION	EXPLANATION
LAN	Local Area Network
LIS	Laboratory Information System
M2M	Machine-to-Machine
MAC	Media Access Control
mHealth	Mobile Health
MISP	Malware Information Sharing Platform
MRI	Magnetic Resonance Imaging
MS	Member State
NAC	Network Access Control
OS	Operating System
PACS	Picture Archiving and Communication System
PCSP	Primary Care Service Provider
PHR	Patient Health Record
PIS	Pharmacy Information System
PKI	Public Key Infrastructure
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
ReEIF	Refined eHealth European Interoperability Framework
RIA	Research and Innovation Action
SMART	Simple, Measurable, Actionable, Relevant and Time-based
SMB	Server Message Block
SQL	Structured Query Language
SSID	Service Set Identifier
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UC	Use Case
UDP	User Datagram Protocol
USB	Universal Serial Bus
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WP	Work Package
WPA2	WiFi Protected Access II
XSS	Cross-site scripting

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

1.1 Purpose & Scope

This document, named "*Use Cases Definition and Pilot Overview Document v3*", is elaborated as part of Task 2.4 - Reference Scenarios and Pilot Operations Specifications and KPIs and presents the final version of the SPHINX application scenarios and use cases (UC). Whereas the application scenarios address the new healthcare landscape crafted by the digital transformation of systems, processes and organisations, the use cases describe representative situations concerning cybersecurity incidents (attacks) affecting the healthcare assets. The cybersecurity incidents herein address healthcare providers (e.g., hospitals and care centres) as well as industry and services' providers (e.g., IT providers, medical device manufacturers, security consultants), identifying a list of preventative and mitigation measures to safeguard critical healthcare assets and reduce potential negative impact. The application scenarios and use cases are the foundation for understanding and defining the SPHINX system, from a functional and technical perspective, as well as the SPHINX pilots aiming to test and validate the SPHINX system in real-life conditions, in order to ascertain its contribution to assess and reduce cyber risks in healthcare organisations so as to protect privacy, data and infrastructures. Importantly, the use cases facilitate the understanding of the added-value of the SPHINX toolkit in relevant cyber incident situations, allowing for the clarification of the benefits and positive impact brought by SPHINX.

1.2 Structure of the Deliverable

This document is structured as follows: section 1 introduces the document; section 2 establishes a common setting to address application scenarios and use cases, based on key aspects such as healthcare critical assets, threat taxonomy, threat actors, attack vectors and the overall impact of the attacks; section 3 presents the application scenarios for SPHINX involving the widespread adoption of eHealth and mobile health systems and their contribution to the increased vulnerability of healthcare organisations, their systems, infrastructure and data; section 4 presents the SPHINX use cases, building on the application scenarios and describing relevant cybersecurity incidents in the healthcare domain, including aspects such as attack vectors, areas of vulnerability/exploitation, assets affected and expected impact. Importantly, each incident describes the benefits expected by adopting SPHINX; section 5 introduces the SPHINX pilots, cross-referencing them with pertinent use cases and defining a set of key performance indicators (KPIs) supporting a sound assessment of the SPHINX system's performance, impact and added-value benefits; finally, section 6 concludes the document.

1.3 Relation to other WPs & Tasks

Deliverable D2.9 builds on the previous deliverable versions (D2.4 and D2.7) and takes into consideration the work unfolding across the technically-oriented work packages 3 through 6, related with the development of all the SPHINX System's tools.

The creation of the SPHINX application scenarios and use cases incorporates valuable inputs from Task 2.1 (Cyber Situation Awareness Trend Analysis), namely with respect to the vulnerability and threat landscape in healthcare, to the IT infrastructure layers' attack attribution and to cybersecurity standards and best practices. As a result, application scenarios and use cases refer to prevalent attack vectors, existing vulnerability and exploitation areas and preventative and mitigation techniques.

Other relevant contributions proceed from Task 2.2 - Basis of Legal and Ethical Requirements, concerning the ethical and legal requirements to be considered in the design, development and deployment of the SPHINX system, including its data protection and trusted services; as well as from Task 7.1 - Site Surveys and Planning of Pilot Operations, involving the presentation of SPHINX pilot plans and the definition of the evaluation framework to assess the performance of the SPHINX System.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

On its turn, this document delivers valuable inputs to the tasks defining stakeholders' requirements (Task 2.3) and the SPHINX technical architecture (Task 2.5), as it lays the basis to capture user requirements and establish technical specifications. In this context, Deliverable D2.9 also provides guidance towards the technical implementation to be performed in WPs 3 through 5. Finally, this document serves the guidelines for the work to setup, conduct and validate the SPHINX pilot activities within WP7.

1.4 Methodology

To perform the analysis of the healthcare domain and produce the SPHINX application scenarios and use cases presented in this deliverable, the SPHINX partners participating in Task 2.4 have based their methodological approach in the Common Criteria for Information Technology Security Evaluation (CC) model, which is an international standard for computer security certification (ISO/IEC 15408) ensuring that the evaluation of Information Technology (IT) products is performed in accordance to high and consistent standards [1, 2, 3].

At the basis of the work carried out in Task 2.4 is the general model of the CC model, establishing the concepts of countermeasures, assets, risks, threats and threat agents:

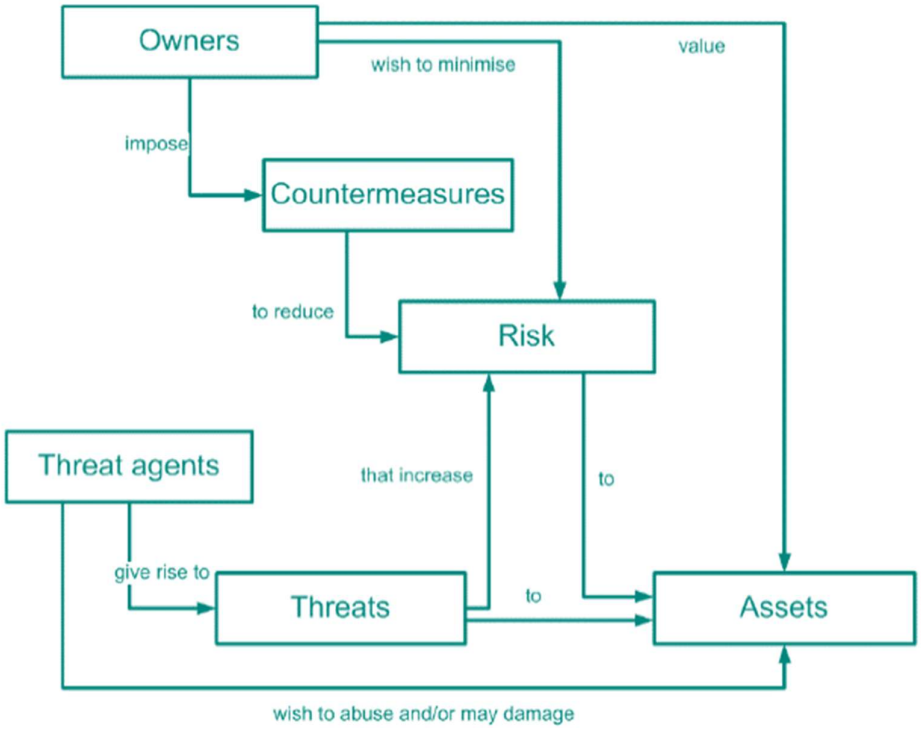

Figure 1: General Model of Concepts and Relationships from Common Criteria Part 1

Because the SPHINX RIA will not produce a market-ready deployable version of the SPHINX System (this result will exhibit a Technology Readiness Level of 7 at the end of the SPHINX RIA), it has been decided to adapt the CC model to the specifics of the SPHINX Action (namely the absence of a full-developed product. Consequently, complying with the CC method, the work performed in Task 2.4 and described in this deliverable comprise the following activities:

1) Consider the healthcare ICT ecosystem and identify the critical assets to protect, the threat taxonomy, the involved threat actors, the prevalent attack vectors and the associated impact of the cybersecurity incidents;
2) Create the SPHINX application scenarios;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3) Derive the SPHINX use cases, portraying specific security risks or threats to the critical healthcare assets to protect and establishing the adequate security controls and processes delivered by the SPHINX system to prevent, handle and mitigate the occurrence of the identified threats;

4) Present the SPHINX pilots, cross-referenced to the SPHINX use cases, and define the applicable requirements and key performance indicators (KPIs);

5) Analyse, review and mature the SPHINX use cases to ensure they meet the applicable user requirements and expectations, while accurately illustrating the benefits of adopting all SPHINX tools.

To support the work performed in Task 2.4 and the production of this deliverable, the SPHINX partners combined literature analysis and online specialised research sources with their own expertise on cybersecurity, benefiting from the participation of the partners' IT cybersecurity officers with extensive practical know-how in implementing security measures and dealing with cyberattack recovery and mitigation. External stakeholders' feedback is also incorporated resorting to online questionnaires and feedback received from the SPHINX "Cyber Situation Awareness trend" Workshop.

As key references, the SPHINX partners abide to the approach set forth by the European Union Agency for Network and Information Security (ENISA) (https://www.enisa.europa.eu) on attack scenarios and eHealth use cases:

- ENISA Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures. November 2016 [4];
- ENISA Security and Resilience in eHealth - Security Challenges and Risks. 2015 [5].

Concerning cybersecurity taxonomies, the following sources are used:

- ENISA Reference Incident Classification Taxonomy - Task Force Status and Way Forward. January 2018 [6];
- Malware Information Sharing Platform (MISP) Taxonomy, which compiles several taxonomies including ENISA's Threat Taxonomy [7].

SPHINX deals with developing a cybersecurity toolkit for the healthcare domain, looking into highly connected ecosystems and concepts around the future of healthcare. Thus, the ENISA report on smart health service and infrastructures [4] is used as main reference for the definition of critical healthcare assets, threat taxonomy, threat actors, attack vectors and the associated negative impact, presented and adapted in the following section.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2 Critical Assets, Threat Taxonomy, Threat Actors, Attack Vectors and their Impact in SPHINX

Current state architecture, engineering and operations in cybersecurity focus largely on compliance to one or many regulations, directives, policies or frameworks. Organisations build on these best practices by incorporating traditional information security concepts and principles, aiming to provide security services, detect and respond to threats and incidents, and analyse collected data to identify trends and patterns in order to improve existing security controls and services.

This section addresses the basic concepts of cybersecurity allowing the SPHINX Consortium to define reference scenarios and use cases in healthcare and deliver well-representative pilots. The key concepts considered are critical assets, threat taxonomy, threat actors, attack vectors and the associated impact presented next.

2.1 Critical Healthcare Assets

Assets represent any resource that is worth protecting, for example data, components, functionality, services, people or physical resources. In SPHINX, and based on [4], the following critical healthcare assets are considered:

1) **Healthcare information systems**: the digital administrative and clinical systems, applications and services supporting the activity of the healthcare service provider, both stored locally and accessed remotely (for example, national healthcare databases), including the Administrative and Billing System, the Patient Admission System, the Remote Patient Monitoring System, the Telemedicine System, the Laboratory Information System, the Radiology Information Systems, the Picture Archiving and Communication Systems, the Electronic Health Records, the ePrescription service and the eProcurement service;
2) **Healthcare data repositories**: the different databases in each healthcare service provider where information is stored locally;
3) **Identification system**: the system used to perform authentication of users, including patients and staff, and of equipment (e.g., beds, radiology scanners, blood analysers).
4) **Networked medical devices**: a set of medical equipment integrated in the healthcare service provider's IT network to support the delivery of care;
5) **Mobile user devices**: a set of user devices (tablets, smartphones, wearables) interacting with the healthcare service provider's IT network to ensure the creation of new points of care (e.g., at home) and that the right information is available at the right place at the right time and to facilitate the mobility of staff and patients;
6) **IT and networking equipment**: infrastructure components enabling access to healthcare information systems (e.g., desktop computers and servers) and providing the connectivity backbone that connects them (e.g., routers and gateways);
7) **Healthcare data**: the informational resources at the centre of all medical decision-making processes to support high-quality healthcare services;
8) **Buildings and facilities**: the physical resources that are critical for the operation of the healthcare service provider, including servers, data centre, heating system, elevators, oxygen distribution.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.2 Threat Taxonomy

A taxonomy is defined as a classification of terms that facilitates the understanding of a given reality. According to ENISA, three characteristics define a taxonomy [8]:

- a form of classification scheme to group related things together and to define the relationship these things have to each other;
- a semantic vocabulary to describe knowledge and information assets; and
- a knowledge map to give users an immediately grasp of the overall structure of the knowledge domain covered by the taxonomy, which should be comprehensive, predictable and easy to navigate.

In SPHINX, and based on [4] and [7], the following threat taxonomy is considered:

1) **Malicious actions**: Malware, Hijacking, Medical device tampering, Social engineering attacks, Device and data theft, Phishing, Denial of Service (DoS)/Distributed DoS (DDoS);
2) **Human error**: Medical system configuration error, Absence of audit logs, Unauthorised access control, Non-compliance to security procedures (e.g., Bring Your Own Device or BYOD), User error;
3) **System failure**: Software/firmware failure, Device failure, Network component failure, Legacy or obsolete systems, Outdated systems, Insufficient maintenance, Overload;
4) **Supply chain failure**: Cloud service provider, Medical device manufacturer, Network provider, Power supplier, Information system manufacturer, Services supplier;
5) **Natural phenomena**: Earthquakes, Flood, Fires, Heavy storms.

2.3 Threat Actors

A threat actor or malicious agent is a person or entity that is responsible for an event or incident that impacts, or has the potential to impact, the safety or security of critical assets. From a threat intelligence perspective, threat actors are often categorised as [9, 10]:

- **Government Sponsored**: These groups are well funded and often build sophisticated, targeted attacks motivated by political, economic, technical or military agendas. Often, they look for competitive information, resources or users that can be exploited for espionage purposes;
- **Organised Crime**: Cybercriminals who engage in targeted attacks driven by profits. They typically look for critical digital resources that have high value on the black market, such as personally identifiable information (PII), social security numbers, health records, credit cards and banking information, to hijack and ransom;
- **Cyber Terrorists**: Politically motivated extremist groups that use cyber techniques to intimidate, coerce, or influence an audience, force a political change or cause fear or physical harm. They use the Internet more as a recruiting and propaganda means of communication to extend the traditional terrorism into cyberspace. However, they exhibit the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Their actions, more often than not, have no lasting effect on their targets beyond reputation;
- **Hacktivists**: Attackers with a political agenda, who long for high-profile attacks to help them gain awareness to their cause (distribute propaganda) or benefit their cause, by causing damage to organisations they are opposed to;
- **Opportunistic**: Attackers who are amateur criminals, often referred to as script kiddies, driven by the desire for notoriety. They may become legitimate security researchers trying to help organisations find and close security vulnerabilities, or even professional hackers looking to profit from finding and exposing flaws and exploits in network systems and devices;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- **Insider Threat**: Attackers operating within the organisation, who are typically disgruntled employees or ex-employees looking for revenge or financial gain. Inside actors often have direct access to sensitive data but also knowledge about internal operations and processes. On top of that, their activity is much less likely to trigger a red flag within the network and various tools network intrusion tools, like firewalls, are ineffective against inside threats.
- **Internal Users**: Internal actors who are simply negligent or careless, making mistakes with configurations that may bring down critical resources such as firewalls, routers, and servers, causing widespread outages. They represent the largest threat organisations face, created largely due to network design flaws or by the wrong assignment of privileges or access. Insiders often become unwitting participants in attacks because outside actors use social engineering and other techniques to obtain insider credentials and compromise the organisation with legitimate user credentials.

In SPHINX, and based on [4], the following threat actors are considered:

1) **Insider threats**: These are threat actors operating within the healthcare organisations, namely employees and suppliers, that have a malicious intent to disrupt the healthcare service delivery by causing harm to the organisation's ICT systems. These can be potentially the most harmful threat actors in place, ranging from physicians, nurses, administrative staff to third-party suppliers (cleaners, security guards, catering suppliers);
2) **Malicious external users**: These threat actors are a part of the healthcare organisation's ecosystem, namely patients and their visiting guests, that have a malicious intent to disrupt the healthcare service delivery by causing harm to the organisation's ICT systems. Because of their privileged access to the healthcare organisation's critical assets, these actors' malicious actions can cause great impact;
3) **Remote attackers**: These threat actors include amateur and professional criminals that, while not physically present at the healthcare organisation's facilities, are able to exploit vulnerabilities within the healthcare service provider's interconnected health ecosystem and gain access to the overall ICT system to disrupt the healthcare service delivery for profit and personal notoriety;
4) **Others**: These threat actors refer to natural causes leading to equipment and system failures.

2.4 Attack Vectors

An attack vector is "a path or means by which a threat agent can gain access to a computer or network server, abuse weaknesses or vulnerability on assets (including human) in order to achieve a specific outcome" [11]. In SPHINX, and based on [4], the following attack vectors are considered:

1) **Physical interaction with IT assets**: Attackers that are physically present within the healthcare facilities and are able to directly interact with the existing equipment, devices and systems that they have access to, including networked medical devices or interconnected clinical information systems (smart pharmacy storing booth);
2) **Wired communication with IT assets**: Attackers that are physically present within the healthcare facilities and gain access to the healthcare service provider's IT assets through the use of wired network communications (including access to the Internet), including cloud services, connected medical devices and online healthcare information systems (drug inventory, patient health database).
3) **Wireless communication with IT assets**: Attackers that may either be physically present within the healthcare facilities or remotely located and gain access to the healthcare service provider's IT assets through the use of wireless technologies, including identification systems or mobile devices;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4) **Interaction with users**: Attackers that privilege social engineering attacks (focus on users with privileged access) to gain access to the healthcare service provider's IT assets. These attacks may either involve directly fooling or convincing the users to relinquish such access (share login credentials or passwords, provide keys) or reflected attacks, such as Cross-site scripting (XSS) or Cross-Site Request Forgery (CSRF), by which the attacker sends a link via email or chat, leading the user to click on it and thus activate malicious code capable of hijacking the user's access and intentionally harm the healthcare service provider's critical assets.

2.5 Impact Caused by Cybersecurity Incidents

Any security incident affecting critical assets cause severe impact in the regular functioning of systems, services and applications, to the benefit of society. In the healthcare domain, the systems' availability, interoperability, access control and authentication, as well as the high privacy and confidentiality requirements of healthcare data represent key security challenges that, in case of failure to deliver adequate security, disrupt the overall healthcare service delivery to the general population.

In SPHINX, and based on [5], the following impacts are considered:

1) **Loss of availability**: the absence of access to (classified) healthcare information or to application services or to information exchange between point of care sites;
2) **Data integrity violation**: the absence of quality, accuracy and consistency of the data stored and exchanged for clinical and administrative purposes;
3) **Data confidentiality violation**: the unmonitored or illegal access to or misuse of sensitive healthcare information.

These service outages affect significantly the healthcare service delivery, the trust in the healthcare industry and the safety of patients, leading to unnecessary duplication of tests and investigations and the increase of healthcare service delivery costs, as well as to serious distress to the society.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3 Application Scenarios for SPHINX

Cybersecurity is an increasingly critical aspect of healthcare information technology infrastructure. Nowadays, the use of automation and information and communication technologies has generated unprecedented volumes of healthcare information and a regular connection between patients and the responsible healthcare professionals, as well as the integration of connected medical devices and user equipment and the coexistence of healthcare information systems of diverse nature, including many outdated legacy applications and systems. Above all, the healthcare industry can expect the use of digital technology to continue to proliferate across multiple channels. The convergence of personal health and consumer technology will create an *Internet of medical things*, requiring local, regional and national threat prevention strategies.

In this context, the rapid digitisation of healthcare delivery, from electronic health records and telehealth to mobile health (mHealth) and network-enabled medical devices that constitute a broad cyber surface, introduces risks related to cybersecurity vulnerabilities that are particularly worrisome because cyberattacks in a healthcare setting can result in the exposure of highly sensitive personal information, cause disruptions in clinical care or affect the safety of patients, for example, by compromising the integrity of data or impairing medical device functionality. The threat is real and growing in tandem with the pace of industry digitisation. Yet cybersecurity capacities currently remain behind the pressing needs, lagging behind the robust pace of adoption of digital networks by threat actors. This disconnect places the multitrillion-dollar healthcare sector at risk of even more significant cyberattacks.

Indeed, healthcare organisations are particularly vulnerable to cyber threats. Verizon's 2018 Data Breach Investigation Report found that the healthcare field, in general, was most affected by data breaches, which accounted for 24% of all investigated breaches across all industries [12]. Additionally, a report by the Ponemon Institute found that almost 90% of respondents involved in health plans and health care clearing houses as well as health care providers with electronic health records experienced a data breach in the past 2 years [13]. The causes are multifactorial, involving both technology and people, and human error and cultural factors play increasingly critical roles. Despite efforts to teach best-practice security behaviour through training programs, recent surveys reveal that one in five healthcare employees still write down their usernames and passwords on paper [14].

The application scenarios for SPHINX focus the adoption of innovative information and communication technologies by healthcare stakeholders, giving way to national eHealth strategies and a common EU eHealth policy, including healthcare data capture (secure collection of patient data from multiple sources), analysis (data processing and analytics to extract actionable information from captured healthcare data) and sharing (deployment of healthcare information networks that securely retrieve patient data from multiple sources and make it available to the patient and the responsible healthcare professional), in order to improve significantly the delivery of high-quality cost-efficient healthcare via informed decision-making.

Based on [5] and adapted to the specific context of the SPHINX RIA, the application scenarios presented next focus therefore on today's growing digitisation of healthcare information and service delivery and its associated security challenges, all of which addressable through the innovation brought forth by the SPHINX system.

3.1 Digital Transformation in Healthcare

Reflective of an industry facing rapid technological and social change, healthcare is undergoing a digital revolution, driven by the need to increase efficiency, reduce error and overhead in the provision of care and improve patient care.

From a market perspective, healthcare is still comparatively new to digitisation, with the vast majority of related

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

large-scale investments on software and services in frontline clinical and administrative healthcare occurring in the last decade. Throughout the years, rendering administrative processes, clinical pathways and patient data into digital realities has driven a focus on data standardisation, data integration, data security, data storage, and unified desktop technologies that can stitch together disparate system workflows. Adding new computers, servers and devices and creating more dedicated networks has led to a panoply of different operating systems, applications and databases that resulted in each healthcare organisation having unique IT architectures, networks and specialist cybersecurity needs. In a typical organisation, computers, servers and printers multiply, as well as portable devices used in patient rooms and laptops taken home for use after-hours. In the mix, outdated and legacy firmware with unaddressed bugs and known vulnerabilities compound the difficulty to maintain up-to-date security policies, measures and systems, increasing the number of vulnerabilities or risks. Also, with increased digitisation, new privacy regulations and more integration between different systems bring new risks and an increased burden of regulatory compliance.

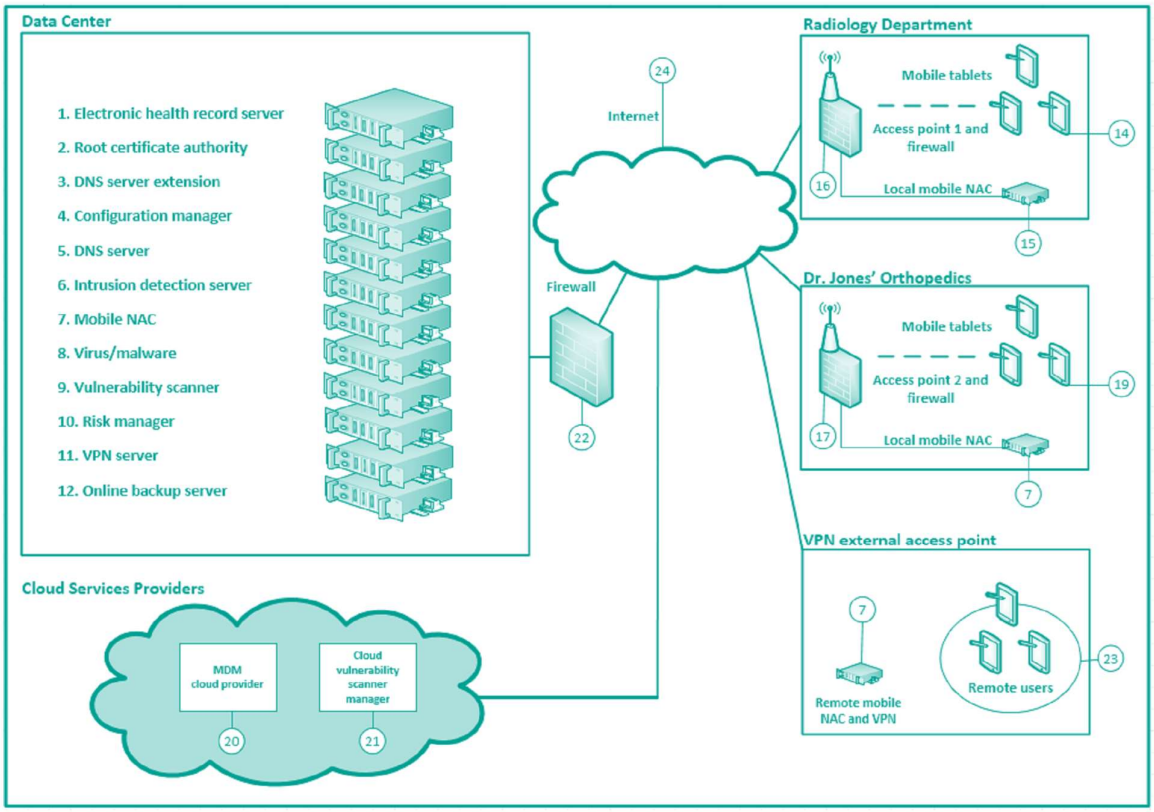

Figure 2: The Digital Healthcare Service (from [15])

Indeed, the current pace, scale and complexity of technology adoption is putting healthcare organisations at a significant risk of multiplying its cyber risks. When it comes to data as sensitive as private health information, the potential for an attack should always be taken seriously for healthcare data has become one of the most desirable premium commodities for sale on black market sites. At a time when data breaches are at an all-time high and organisations are still grasping how to handle these new and improved threats, it does not bode well that cyber-security strategies are often overlooked or neglected, resulting in some healthcare organisations' networks to have significant exposure to threats and a limited ability to detect or resist attacks. Not only do multiple sites require access to patient information across a spectrum of health facilities – such as local clinics, physician offices, hospitals, laboratories and pharmacies – but the information also needs to be readily available

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

to support open new healthcare services, such as allocation of medical practices, second opinion consultation services, comparison of diagnostic protocols or participatory healthcare. Add to this the organisations' willingness to allow their employees to bring their own devices, and it is understandable how extremely challenging it is to implement network-wide security practices and data protection.

The next table lists the critical healthcare assets resulting from the digital transformation of healthcare that are likely to be targeted by a cyberattack:

Asset	Asset Category (see 2.1)
Healthcare Organisation Environment	
Organisation Facilities (e.g. servers, data centre, heating system, elevators, oxygen distribution)	**Buildings and facilities**
Server Computers	**IT and networking equipment**
Desktop Computers (incl. HW, OS and supporting SW)	**IT and networking equipment**
Network devices (e.g., public and restricted routers/AP) and Gateways (internal-external network)	**IT and networking equipment**
IT Security Systems (e.g., firewall, anti-virus, backup system, access control, authentication system, PKI)	**Healthcare information systems**
Organisation Management Systems and Databases (e.g., HR systems, payment system, billing system, inventory and stock system, appointment system, pharmacy system)	**Healthcare information systems Healthcare data repositories**
Patient Data	**Healthcare data**
National or Regional Healthcare Databases Client Access Service	**Healthcare information services**
BYOD (e.g., portable computers, tablets, mobile phones)	**Mobile user devices**

Table 1: Relevant Healthcare Assets in the Digital Transformation in Healthcare Application Scenario

Application Scenario Challenges

This application scenario especially illustrates the following challenges in healthcare delivery:

- To deal with digitised healthcare databases and services;
- To deal with outdated (legacy) operating systems, applications and databases;
- To deal with the integration of healthcare and patient data from multiple databases;
- To deal with the availability, integrity and confidentiality of healthcare and patient data;
- To deal with the users' authentication and profile management;
- To deal with the integration of BYOD devices in the healthcare organisations' networks.

The Digital Transformation in Healthcare is a common application scenario across Europe. For healthcare ecosystems to remain safe from cyber exploitation, cybersecurity strategies need to move beyond servers and desktops to reflect a world of interconnected networks, equipment, devices and users.

3.2 eHealth Services

Supported by the Connecting Europe Facility (CEF) Telecom programme, EU Member States are working on an eHealth Digital Service Infrastructure under the aegis of the eHealth Network, the network of national authorities responsible for eHealth (2011/890/EU). In addition to Finland, Greece, Italy, Portugal, Spain, France, Denmark, Estonia and Czech Republic, 18 countries are expected to exchange Electronic patient summaries and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

ePrescription by the end of 2021.

Healthcare organisations are gradually adopting new technologies to deliver nation-wide healthcare services online (eHealth), such as ePrescription/eDispensation, Electronic patient summary, eReferrals and eBilling, that significantly facilitate the interaction of citizens and patients with healthcare organisations, as well as the daily work of thousands of healthcare professionals and employees.

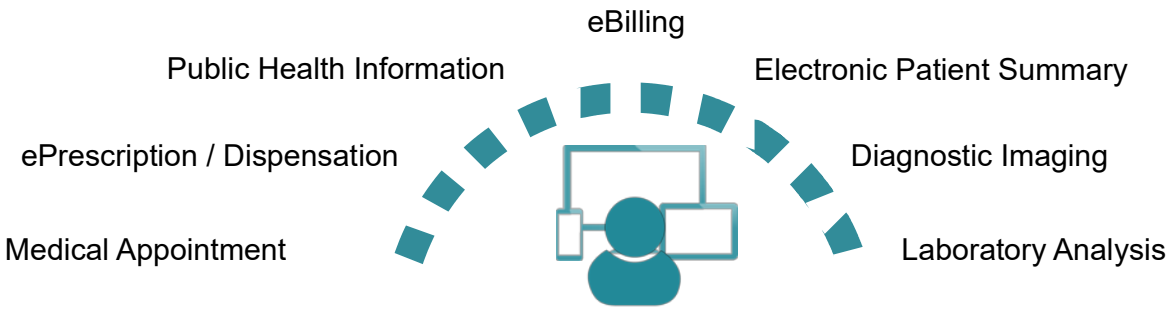

Figure 3: eHealth Services

Based on transactional processes dealing with added value services, eHealth services have become the cornerstone of many national or regional health IT strategies as healthcare professionals need an accurate and actual overview of the patient's continuity of care record and specific administrative or medical procedures that are distributed in more than one point of care setting.

In this regard, organisation implementing eHealth services are adopting widely used Internet-based technologies (e.g., IP and web services) and open standards (e.g., HL7) allowing access from commodity devices (e.g., mobile phones and web-browsers) for users and services (intra and extra organisation). Herein, organisations need to expose resources to external entities where security controls cannot be enforced.

As healthcare organisations try to keep pace with the latest online technologies and eHealth services, offering the potential of improved care and more efficient patient management, an array of vulnerabilities is exposed and bring heightened concerns regarding privacy and security about third-parties' risks, inappropriate releases of sensitive and private information from healthcare records and the systemic flows of information throughout healthcare organisations.

In this environment, healthcare organisations still need to deliver trusted eHealth services, that is, provide reliable information and transactions while assuring confidentiality and privacy.

Online healthcare services need to implement robust and reliable authentication and verification mechanisms preventing risk of data breach (e.g., illicit access to sensitive data) or fake transactions (e.g., abuse medical prescriptions and collect payments from eBilling), especially considering automated exchanges (M2M). Moreover, services need to have resilience in mind in order to overcome attacks, such as denial of service.

As healthcare systems increasingly rely on web-enabled eHealth services and online transactions for care delivery, they also become more vulnerable to cyberattacks, requiring appropriate cybersecurity policies and solutions.

The next table lists the critical healthcare assets on eHealth services that are likely to be targeted by a cyberattack:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Asset	Asset Category (see 2.1)
Healthcare or Service Provider Organisation Environment	
Organisation Facilities (e.g. servers, data centre, heating system, elevators, oxygen distribution)	**Buildings and facilities**
Server Computers	**IT and networking equipment**
Network devices (e.g., public and restricted routers/AP) and Gateways (internal-external network)	**IT and networking equipment**
IT Security Systems (e.g., firewall, anti-virus, backup system, access control, authentication system, PKI)	**Healthcare information systems**
Web eHealth services and databases (for e.g., ePrescription, eDispensation, eProcurement, Patient records, Referrals)	**Healthcare information systems** **Healthcare data repositories**
Patient Data	**Healthcare data**
Patient/User Environment	
Patient/User Desktop Computers (incl. HW, OS and supporting SW)	**IT and networking equipment**
Automated M2M Service Exchange	**Healthcare information systems**
Patient/User Network devices (e.g., Wi-Fi Router/AP)	**IT and networking equipment**
Patient/User BYOD (e.g., tablet, smartphone)	**Mobile user devices**

Table 2: Relevant Healthcare Assets in the eHealth Services Application Scenario

Application Scenario Challenges

This application scenario especially illustrates the following challenges in healthcare delivery:

- To deal with untrusted environments and devices;
- To deal with web-based online healthcare services;
- To deal with exposing web-services to external entities;
- To deal with the availability, integrity and confidentiality of healthcare and patient data;
- To deal with the users' authentication and profile management.

With healthcare data breaches on the rise, healthcare organisations are committed to understand the perceived risks of eHealth services and the security and privacy measures patients expect, so they can begin to diagnose and overcome the barriers to adopting and embracing eHealth services.

3.3 mHealth and Remote Patient Monitoring Platforms

Mobile health (mHealth) supports the delivery of healthcare via remote access medical devices, IoT-based health devices (the Internet of Medical Things or IoMT) and mobile applications that connect to healthcare IT systems through computer networks, empowering the sharing of health and wellbeing information, enabling the shifting of healthcare to a more preventative care outside of the hospital environment, giving rise to services such as telehealth (video appointments and consultation) and remote patient monitoring platforms, and delivering high-quality healthcare.

Experts estimate that there will be more than 64 billion IoT devices by 2025 [16], and a significant portion of these will be medical devices, from heart monitoring implants and pacemakers to infusion pumps, mobile medical workstations, in-home monitors and personal fitness devices or wearables. According to a study conducted by the McKinsey Global Institute, spending on the Healthcare IoT solutions will reach $1 trillion by

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2025 [17]. Currently, 3 million patients worldwide are connected to a remote monitoring device that performs routine tests – such as checking glucose levels for patients with diabetes or checking blood pressure for patients receiving cardiac care – and sends personal medical data to their healthcare provider [18].

Remote medical and health devices hence allow healthcare professionals to closely follow patients outside of the office, either through telehealth (video consultation) or remote patient monitoring. Some of these devices only send information via a wireless connection, like a pacemaker, while others can send and receive information, like infusion pumps. The use of personal health monitoring devices and smartphone applications (Apps) is also on the rise. Most of these devices are connected to patient remote monitoring Apps that focus on the collection of patient-generated health data from home, through devices and mobile health platforms that connect via the patient's home network or cellular network, to the primary care provider or care team. This data can either be collected and sent by the patient or gathered by connected devices and sent to the provider without requiring the patient's intervention. In this manner, a care professional may use the hospital's platform or the remote patient monitoring App in its own smartphone to monitor a patient around the clock, gathering data on health, activity, diet and exercise, the environment, even social determinants, thus filling out a health record that would otherwise be limited to the patient's visits.

The care professional may also use the remote patient monitoring platform to push health and wellness advice, care management tips and other resources to the patient, based on trends spotted in the patient-gathered data. By creating a more complete record, the care professional can gain a better understanding of a patient's overall health and develop a care plan that more closely adheres to a patient's life. Further, the analysis of the data collected through national (or regional) electronic medical records, diagnostic information gathered through imaging equipment and personal medical and health devices enhances the medical decision-making process and empowers patients to take a more active role in managing their personal health, attaining better health outcomes. With mHealth tools and platforms, telehealth and remote patient monitoring platforms have the potential to extend care management and coordination outside the healthcare organisation and into the patient's home. In addition, the increase of available connected devices in the hospital and home environments provides the opportunity to deliver highly personalised, accessible and on-time healthcare services, reduce the number of visits and hospitalisations, eliminate unnecessary waste, contain healthcare costs and save lives.

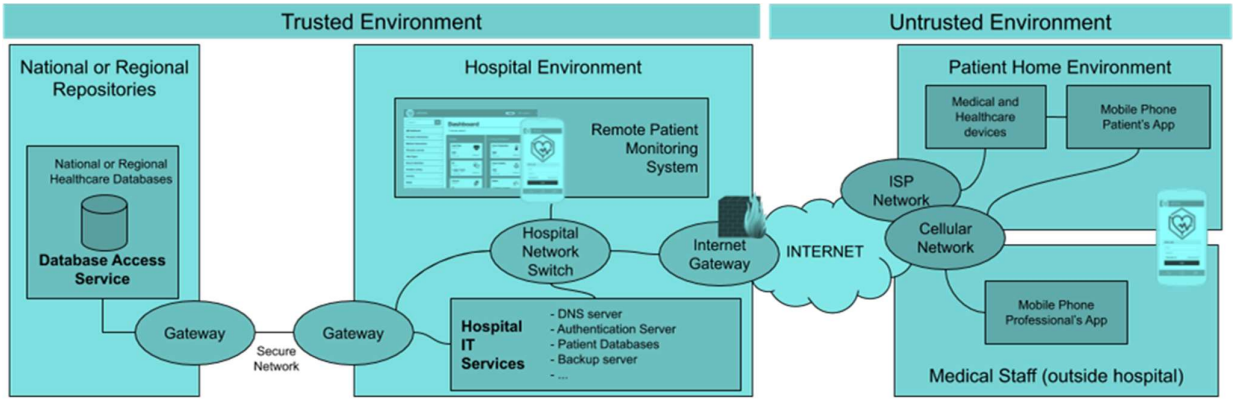

Figure 4: The Mobile Healthcare Service

Indeed, healthcare organisations recognise the value added of mHealth, connected medical and health devices and telehealth and remote patient monitoring platforms to the successful implementation of digitally-connected coordination of care. Nevertheless, in a highly complex environment, these trends stretch the boundaries of cybersecurity, while creating new, often insecure, entry points for hackers and rising data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

security and liability risks.

Not only medical and health remote monitoring devices may be vulnerable to viruses and malware that can compromise the effectiveness of the devices (device failure or malfunction), the patients' privacy and the healthcare organisation's ICT ecosystem, but also the transmission of patient data enabled by those devices represents a risk of data breach if the information is not properly secure. In addition, the increasing use of BYOD (patients' tablets and smartphones) are a potential issue as they may have developed networks and connectivity glitches and may very easily provide an on-ramp for attackers to healthcare networks. Moreover, they are prone to be lost or stolen, which could lead to identity theft and loss of privacy. Since these devices are outside the healthcare organisation's control, there is also a lack of visibility and control over personal devices, as well as the absence of awareness of these devices' vulnerabilities that attackers could take advantage of. As healthcare systems become interconnected, especially as numerous wireless medical devices start connecting to web-enabled IT systems they become increasingly vulnerable. From a cybersecurity perspective, healthcare organisations need to rethink medical and health device management and consider all the variables this mobile technology introduces, compared to traditional workstations and laptops.

The next table lists the critical healthcare assets that are likely to be affected by a cyberattack on connected medical and health devices and telehealth and remote patient monitoring platforms:

Asset	Asset Category (see 2.1)
Healthcare Organisation Environment	
Healthcare Organisation Facilities (e.g. servers, data centre, heating system, elevators, oxygen distribution)	**Buildings and facilities**
Server Computers	**IT and networking equipment**
Desktop Computers (incl. HW, OS and supporting SW)	**IT and networking equipment**
Network devices (e.g., public and restricted routers/AP) and Gateways (internal-external network)	**IT and networking equipment**
IT Security Systems (e.g., firewall, anti-virus, backup system, access control, authentication system, PKI)	**Healthcare information systems**
National or Regional Healthcare Databases Client Access Service	**Healthcare information services**
Remote Patient Monitoring System	**Healthcare information systems**
Patient Databases	**Healthcare data repositories**
Remote Patient Monitoring App for Professionals	**Healthcare information systems**
BYOD (e.g., portable computers, tablets, mobile phones)	**Mobile user devices**
Patient/User Environment (at Home)	
Home	**Buildings and facilities**
Patient/User Home Network devices (e.g., Wi-Fi Router/AP)	**IT and networking equipment**
Medical Devices	**Networked medical devices**
Healthcare Devices (IoT)	**Mobile user devices**
Patient/User BYOD (e.g., tablet, smartphone)	**Mobile user devices**
Remote Patient Monitoring App for Patients	**Healthcare information systems**
Patient/User Data	**Healthcare data**

Table 3: Relevant Healthcare Assets in the mHealth and Remote Patient Monitoring Platforms Application Scenario

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Application Scenario Challenges

This application scenario especially illustrates the following challenges in healthcare delivery:

- To deal with untrusted environments and devices;
- To deal with remote healthcare services (in-home care), such as telehealth consultations and remote patient monitoring platforms;
- To deal with the integration of IoT-enabled medical and health devices in the healthcare organisations' networks;
- To deal with the integration of patients' BYOD devices in the healthcare organisations' networks;
- To deal with the availability, integrity and confidentiality of healthcare and patient data;
- To deal with the users' authentication and profile management.

With the development of the *smart home* concept, the Internet of Medical Things and the advent of better mHealth technology, telehealth and remote patient monitoring platform stand to become an accepted standard of high-quality healthcare delivery for the 21st century.

3.4 Sharing and Exchange of Healthcare Information

The introduction of digital technologies in healthcare organisations has enabled the transition from paper-based health records to electronic health records (EHRs) and patient health records (PHRs). Part of comprehensive patient care, EHRs are the systematic collection of a citizen's health history and status, administrative and financial information, to establish the patient care information, created, used, stored, retrieved and located in a healthcare setting by healthcare professionals for purposes of planning patient care, documenting the delivery of care and assessing the outcomes of care. PHRs contain the same type of information as EHRs — diagnoses, medication, immunisations, family medical histories and provider contact information — but are designed to be set up, accessed and managed by patients. EHRs/PHRs are therefore understood as milestones in national and regional eHealth roadmaps and currently such services are either operational (for example, in Luxembourg, Denmark, Finland, Estonia, France, Romania and Portugal) or under development (for example, in Greece, Cyprus and Italy).

Before the wide-scale adoption of EHRs/PHRs, access to healthcare information entailed paper records, in-person requests to health information management offices and the payment of fees. The increasing digitisation of health records has improved access to health information, with healthcare professionals being able to easily access and view diagnosis, medication history, clinical decision support notes, lab results, imaging, treatment plans and post-treatment monitoring. In this context, EHRs/PHRs act as pillars of point of care information systems, facilitating not only the follow-up of patients by different healthcare organisations, whether primary care, specialist care or urgent care, and the transfer of patients between healthcare organisations, namely hospitals, but also the sharing and exchange of health information among healthcare stakeholders, such as healthcare providers, pharmacies, insurance companies and researchers. Importantly, data sharing and exchange is essential for ensuring that best practices for improved patient care are shared among healthcare organisations.

As such, EHRs/PHRs are gradually gaining recognition as critical information infrastructures while they acquire and reuse healthcare information, assisting healthcare organisations transition to value-based care. On their part, citizens/patients understand the necessity for health information sharing and exchange and view it as a desirable addition to their care, due to its potential benefit in avoiding medication errors, reducing readmissions and preventing duplication of tests and exams. Currently, the ability of European citizens to access their electronic medical records across the EU varies from one country to another. Although some citizens may access part of their electronic health records at national level or across borders, many others have limited digital

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

access or no access at all. For this reason, the European Commission is working to facilitate access across borders to healthcare data that is secure and in full compliance with the General Data Protection Regulation (GDPR). The recommendation is for EU MS to extend this work to three new areas of the health record, namely to laboratory tests, medical discharge reports and images and imaging reports. In parallel, the initiative paves the way for development of the technical specifications to be used to exchange health records in each case.

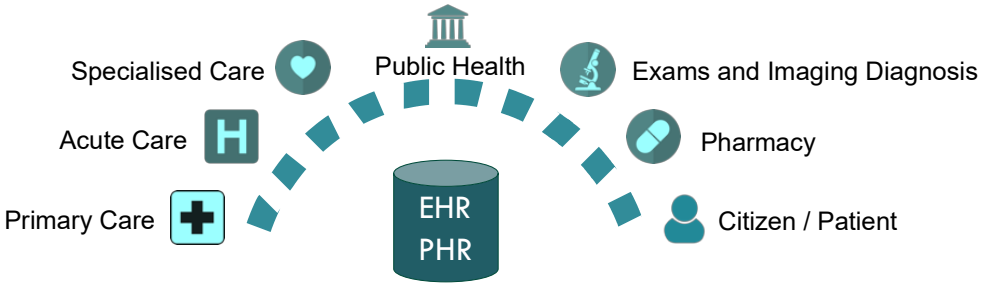

Figure 5: Healthcare Information Exchange

Highly important for the EHRs/PHRs operations are interoperability standards and well-established integration profiles (adopted as EU standard specifications under the 1025/2012 EU regulation), allowing the services to be provided to the appropriate users, across a variety of IT systems, diverse levels of sophistication and interoperable capabilities, a legal landscape of varying degrees and various levels of privacy and rules, ensuring data availability, integrity, non-repudiation, resilience and privacy. Healthcare organisations need to be knowledgeable of the EU and national regulations and requirements with regard to healthcare interoperability, ensuring that they remain compliant to further healthcare data sharing and exchange so that the clinical or operational purpose and meaning of the data is preserved and unaltered. Data security is also a top interoperability priority. Ensuring privacy and the security of the health information throughout the entire data exchange process is a key component to building the trust required to realise the benefits of health information sharing and exchange. As such, access to data needs to be well defined and controlled (e.g., who can access, for how long) and performed operations (e.g., read, modify, delete) must supporting detailed auditing. It is also paramount to ensure data integrity throughout the complete workflow and data lifetime, clearly generating alerts if otherwise.

Along with improving health data security, it is important to consider patient preferences in how their data is handled, allowing them to understand how their information is used and how they could assert more control over which information is shared. Also, healthcare professionals should be aware of the security measures needed to protect their patient data.

The next table lists the critical healthcare assets that are likely to be affected by a cyberattack related with sharing and exchange of healthcare data:

Asset	Asset Category (see 2.1)
Healthcare Organisation Environment	
Healthcare Organisation Facilities (e.g. servers, data centre, heating system, elevators, oxygen distribution)	**Buildings and facilities**
Server Computers	**IT and networking equipment**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Asset	Asset Category (see 2.1)
Desktop Computers (incl. HW, OS and supporting SW)	**IT and networking equipment**
Network devices (e.g., public and restricted routers/AP) and Gateways (internal-external network)	**IT and networking equipment**
IT Security Systems (e.g., firewall, anti-virus, backup system, access control, authentication system, PKI)	**Healthcare information systems**
Web eHealth services (for e.g., ePrescription, eDispensation, eProcurement, Patient records, Referrals)	**Healthcare information systems**
Databases (e.g., EHR and PHR)	**Healthcare data repositories**
Patient/User Data	**Healthcare data**
National or Regional Healthcare Databases Client Access Service	**Healthcare information services**
National or Regional Health Authorities Environment	
Organisation Facilities (e.g. servers, data centre, heating system, elevators, oxygen distribution)	**Buildings and facilities**
Server Computers	**IT and networking equipment**
Network devices (e.g., public and restricted routers/AP) and Gateways (internal-external network)	**IT and networking equipment**
IT Security Systems (e.g., firewall, anti-virus, backup system, access control, authentication system, PKI)	**Healthcare information systems**
Healthcare Databases Access Services	**Healthcare information systems**
National or Regional Healthcare Databases	**Healthcare data repositories**
Patient/User Data	**Healthcare data**

Table 4: Relevant Healthcare Assets in the Sharing and Exchange of Healthcare Information Application Scenario

Application Scenario Challenges

This application scenario especially illustrates the following challenges in healthcare delivery:

- To deal with standardisation and common data exchange formats, complying with EU and national regulations on interoperability;
- To deal with the availability, integrity and confidentiality of patient records and healthcare information across the complete workflow and data lifetime;
- To support detailed auditing on every data operation;
- To deal with the users' authentication and profile management.

The national push for healthcare interoperability continues to gain strength, as a common set of rules for trusted and secure exchange is established between networks across multiple jurisdictions, taking into account applicable legislation, including intellectual property rights, and supporting healthcare organisations in the process.

3.5 Cross-border Healthcare Service Delivery

Cross-border healthcare has been introduced in the EU as required to secure universal quality of service delivered across the Member States, by enabling the flow of healthcare data across borders. Enabling citizens to securely access and share their healthcare data across borders is one of the priorities of the Communication on enabling the digital transformation of health and care in the Digital Single Market. Moreover, the General

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Data Protection Regulation underlines that citizens have the right to access their personal data and provides the legal framework for its protection, setting out directly applicable rules for the processing of the individuals' personal data, including their health data. And rules for facilitating the access to safe and high-quality cross-border healthcare are specifically provided for by the Directive on patients' rights in cross-border healthcare.

The promise of improved quality and continuity of healthcare for citizens and the reduction of healthcare costs by preventing the unnecessary duplication of medical tests and procedures has driven EU-wide efforts by the European Commission and the Member States to facilitate cross-border healthcare service delivery. Under the aegis of the Connecting Europe Facility (CEF) Programme and the eHealth Digital Service Infrastructure (eHDSI), technical specifications for healthcare information exchange were defined, focusing on two sets of health data: Electronic patient summaries and ePrescription. The first exchanges took place between Estonia and Finland in January 2019 and their example will be followed by another 22 EU MS by 2021. With the development and implementation of several EU-funded projects involving standardisation and the exchange of healthcare data in Europe (projects epSOS, EXPAND, Antilope and HITCH), the Refined eHealth European Interoperability Framework (ReEIF) is instrumental to the facilitation of EU-wide healthcare service delivery.

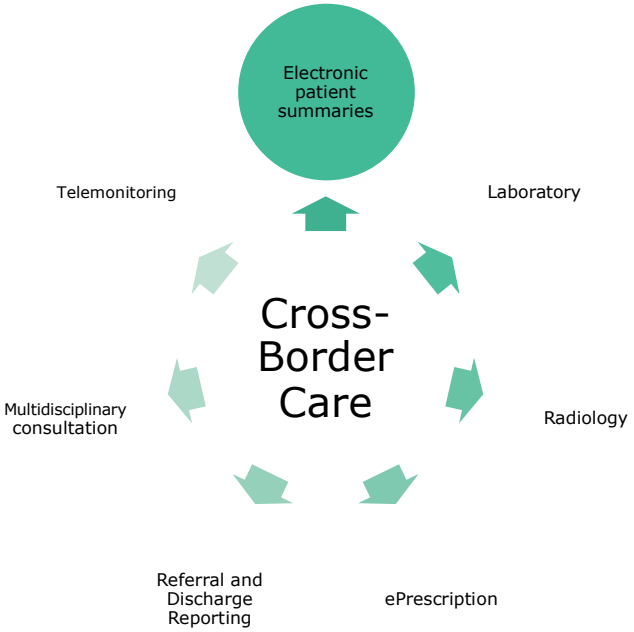

Figure 6: Cross-border Healthcare Service

Currently, healthcare information on specific cases is exchanged among EU MS and Norway through the 24 thematic European Reference Networks (ERNs) that virtually connect 900 highly specialised healthcare units located in 300 hospitals and gather panels of clinicians to diagnose and treat suffering from rare, complex and low prevalence diseases. Healthcare organisations refer patients to the relevant Network, with their consent and upholding existing national regulations, so citizens do not have a direct access to these networks. On the contrary, the digital transformation of healthcare, the creation of eHealth services, the leverage of mHealth and Remote Patient Monitoring platforms and the exchange and sharing of healthcare information, based on the cross-border interoperability of EHRs, PHRs and ePrescription, is focused on the citizen. It will ensure that EU citizens can securely access and exchange their healthcare data wherever they are in the EU.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

On February 6th 2019, the European Commission's Recommendation on a European Electronic Health Record exchange format (C(2019)800) sets the framework to further develop a European EHR exchange format that will enable citizens to securely access and exchange their health data across borders in the EU. The Recommendation establishes a set of common technical specifications for the cross-border exchange of healthcare data and defined the principles to govern, monitor and review this exchange. Further, it underlines the importance of ensuring data protection and security, in line with the GDPR, and full compliance with the cybersecurity framework. A joint coordination process involving the EU MS and the EC is envisaged to conduct this process, engaging relevant stakeholders, including healthcare professional organisations, national competence centres, industry actors and patients' groups, as well as other EU and national authorities.

The next table lists the critical healthcare assets that are likely to be affected by a cyberattack on the cross-border healthcare service delivery:

Asset	Asset Category (see 2.1)
Healthcare or Service Provider Organisation Environment	
Organisation Facilities (e.g. servers, data centre, heating system, elevators, oxygen distribution)	**Buildings and facilities**
Server Computers	**IT and networking equipment**
Network devices (e.g., public and restricted routers/AP) and Gateways (internal-external network)	**IT and networking equipment**
IT Security Systems (e.g., firewall, anti-virus, backup system, access control, authentication system, PKI)	**Healthcare information systems**
National or Regional Healthcare Databases Client Access Service	**Healthcare information services**
Web eHealth services and databases (for e.g., ePrescription, eDispensation, eProcurement, Patient records, Referrals)	**Healthcare information systems** **Healthcare data repositories**
Patient Data	**Healthcare data**
Patient/User Environment	
Patient/User Desktop Computers (incl. HW, OS and supporting SW)	**IT and networking equipment**
Patient/User BYOD (e.g., tablet, smartphone)	**Mobile user devices**

Table 5: Relevant Healthcare Assets in the Cross-border Healthcare Service Delivery Application Scenario

Application Scenario Challenges

This application scenario especially illustrates the following challenges in healthcare delivery in a cross-border scenario:

- To deal with a common vision for EU healthcare service delivery;
- To implement a trusted chain of transactions that ensures data confidentiality;
- To authenticate all involved individuals and IT components (residing in different states);
- To deal with the availability, integrity and confidentiality of healthcare and patient data;
- To deal with standardisation, interoperability and common data exchange formats;
- To deal with different national legislation frameworks on healthcare data.

The national push for healthcare interoperability continues to gain strength, as a common set of rules for trusted and secure exchange is established between networks across multiple jurisdictions, taking into account applicable legislation, including intellectual property rights, and supporting healthcare organisations in the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

process. Built on adequate technical expertise and open standards, the European electronic health record exchange format is set to become the future *de facto* standard for secure cross-border healthcare service delivery across Europe, taking into account full compliance with data protection legislation and ethical principles and abiding to a rigorous cybersecurity framework.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4 Use Cases for SPHINX

This section presents the use cases for SPHINX, inspired in the SPHINX application scenarios and presenting a set of cyber incidents - including associated attack vectors and impact on organisation - in the healthcare domain, in order to better understand the realisation of threats, risks and vulnerabilities and the enabling of improved prevention, recovery and mitigation. Importantly, use cases defined herein facilitate the understanding of the added-value of SPHINX in relevant situations, allowing for the clarification of the benefits and positive impact brought by SPHINX.

The aim of the use cases outlined in this section is to provide a valuable input to frame the definition of the project's SPHINX pilots in section 5. Moreover, they favour a descriptive narrative (easy-to-read and understand) rather than a technically detailed one, in order to be useful for a wide variety of users and stakeholders.

Based on [4], the SPHINX use cases present the following information:

- **Scope**: identification of the applicable scenario as presented in section 3;
- **Attack**: identification of the type of threat, the threat actor(s) and the attack vector(s) as presented in section 2;
- **Vulnerability and exploitation**: identification of the specific vulnerabilities within the healthcare IT ecosystem that have been targeted and exploited by the attacker;
- **Critical healthcare assets**: identification of the healthcare assets affected by the attack and their level of criticality, based on the assets' list presented in section 2;
- **Description**: brief summary of the use case, presenting its rollout and explaining its domain and relevance, referring to the scope, type of attack, areas of vulnerability and exploitation and affected assets;
- **Attack impact**: outline of the negative effects inflicted by the attack, based on the impacts identified in section 2 and considering the healthcare IT ecosystem, the healthcare organisation and key stakeholders, where possible providing estimates of recovery time and potential financial losses;
- **SPHINX role and added-value benefits**: brief description of the role played by the SPHINX system in protecting the healthcare IT ecosystem throughout the attack's timeline, from the prevention phase to the detection, response and recovery phases.

Next, the SPHINX use cases are presented.

4.1 UC1: Attacking Obsolete Operating Systems in Hospital

Use Case 1: Attacking Obsolete Operating Systems in Hospital	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Malicious action – Malware**
Threat Actor(s)	**Remote attackers – Opportunistic**
Attack Vector(s)	**Physical Interaction with IT assets**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 1: Attacking Obsolete Operating Systems in Hospital	
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Legacy and obsolete IT system**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment;** **Healthcare information systems**
Criticality of Affected Asset(s)	**Highly critical**

Table 6: Key Features of the Use Case Attacking Obsolete Operating Systems in Hospital

Use Case Description

Within a hospital facility, the accounting department uses a legacy software application and database that only runs on an obsolete operating system (OS). Running on a virtual machine (VM), this OS has been discontinued (it is no longer supported by its manufacturer) and has known security vulnerabilities. Within the accounting department, all computers have Internet access, which includes the VM that hosts the legacy OS.

The employee uses this VM on a daily basis to performs his work. Occasionally, he also uses the VM to navigate the Internet and accidentally downloads and executes an application infected with a malware (e.g., the *Conficker* malware[1]), thus activating it.

Using spread propagation techniques that exploit vulnerabilities in network protocols, the malware spreads into the hospital's network affecting several connected desktop computers and servers. The malware creates botnets and causes an avalanche phenomenon[2] (e.g., congestion of local network and servers, locking out of user accounts) that renders the hospital's IT infrastructure non-operational. The hospital's information systems exhibit slow response and high latency. Gradually, users cannot log on to their computers and access the hospital's information systems. As the attack spreads, the hospital's medical, nursing and accounting staff are ordered to stop using the digitalised systems and the IT infrastructure and switch to paper-based operations.

Responding to the attack, the hospital's IT department shuts down the whole IT infrastructure and proceeds with a clean installation of computers, resorting to backup systems to partially recover hospital records.

Attack Impact

The use case *Attacking Obsolete Operating Systems in Hospital* directly impacts the hospital's IT infrastructure, causing a **loss of availability** of the existing information systems and services. The attack affects the **healthcare organisation** (the hospital), as operations need to revert to paper-based processes that are highly time-consuming, thus causing significant delays in care delivery. The attack's expected recovery time is estimated to be **2 or 3 working days**, depending on the number of affected assets and on the effort required to re-install the IT infrastructure.

[1] Conficker is a type of computer malware known as a worm that targets a flaw within the Microsoft Windows operating system. Once it infects a computer, it can link the infected computer to a remote computer controlled by the malware author and then download additional instructions to the infected computer. Within an organisation network, Conficker is also capable to spread without user interaction by taking advantage of the protocols computers use to communicate with each other across networks. Conficker is among the largest botnets of the past five years [19].

[2] Certain malwares seek control of infected computers; however, their specific purpose might be configurable during runtime. For example, once installed, the Conficker malware can download additional code instructions, making it a multi-purpose tool.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

SPHINX Role and Added-value Benefits

Dealing with the use case *Attacking Obsolete Operating Systems in Hospital*, the SPHINX System is relevant in the identification of obsolete and vulnerable critical assets (SPHINX vulnerability assessment tool), in the alerting of access to flagged websites (SPHINX data traffic monitoring), in the early detection of the attack by identifying the compromised ports (SPHINX anomaly detection tool), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including recommendations to isolate the compromised assets, block the attack and restore the hospital's IT infrastructure (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Attacking Obsolete Operating Systems in Hospital*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A hospital employee uses a virtual machine with an obsolete operating system.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including operating systems that are obsolete, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	The employee occasionally surfs the Internet using the computer's virtual machine.	
Attack Phase	The employee accidentally downloads and executes a file infected with malware. The malware propagates to several assets in the hospital's network. The malware creates botnets, congests the local network and servers and locks out user accounts. The hospital's information systems exhibit slow response and high latency. And gradually the users cannot log on to their computers and access the hospital's information systems. Hospital's medical, nursing and administrative staff are forced to switch to hardcopy-based operations (paper operations) in order to perform their work activities and deliver care services.	SPHINX detects the access to flagged websites, web traffic and suspicious content (e.g., malicious files). SPHINX recognises the machine's erratic behaviour (e.g., excessive CPU load and traffic), the malicious (botnet) behaviour and traffic (connection attempts to C&C servers, traffic to unusual TCP/UDP ports) SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures. As a result, the IT department is able to isolate the infected assets from the rest of the network, denying the malware access to additional resources and effectively countering malware propagation attempts.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Recovery Phase	The IT department has to proceed with a clean installation of computers (resorting to backup systems to partially recover hospital records).	SPHINX collects relevant attack-related data, including compromised components (e.g., OS, files, protocols), attack patterns, IP packets and remote addresses (IP of the C&C server) and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 7: SPHINX Role and Added-value Benefits in the Use Case Attacking Obsolete Operating Systems in Hospital

4.2 UC2: Hijacking Access to National Healthcare Databases

Use Case 2: Hijacking Access to National Healthcare Databases	
Scope	
Application Scenario	**Sharing and Exchange of Healthcare Information**
Attack	
Threat Type	**Malicious action – Hijacking**
Threat Actor(s)	**Remote attackers – Hacktivists**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Wireless connectivity;** **Unattended legacy systems**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment**
Criticality of Affected Asset(s)	**Highly critical**

Table 8: Key Features of the Use Case Hijacking Access to National Healthcare Databases

Use Case Description

A primary care service provider (PCSP) located in a remote region accesses the national healthcare databases, owned by the National Healthcare Authority, to perform their care service delivery. The national healthcare databases are a well-controlled and protected private network that is part of the National Public Administration Network. However, since the PCSP is remotely located, the access to the national healthcare databases is allowed via the Internet. Hence, to connect to the national healthcare databases, the PCSP uses a wireless ADSL modem/router equipment that has known vulnerabilities.

A hacktivist fakes an injury and is admitted to the PCSP for medical care. While alone, the hacktivist notices an unattended printer and takes the opportunity to gather information about the network interfaces' media access control (MAC) addresses. This information is used to bypass the Network Access Control (NAC) systems, which have MAC address exceptions for legacy printers, and gain access to the PCSP network. Then, the hacktivist scans the network and identifies the ADSL equipment. Aware of its characteristics and vulnerabilities, the hacktivist initiates a password dictionary attack, using default credentials lists freely available on the internet, he is able to find the equipment's password and discovers that all critical modem/router parameters

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

(username, password, Service Set Identifier or SSID, wireless key) remained unchanged from their factory default values. Consequently, the hacktivist accesses the administration interface of the ADSL modem/router equipment, managing to take control of it and effectively breaking the PCSP's connection to the national healthcare databases. In this context, the medical staff is no longer able to access patient medical histories and to prescribe medication.

Responding to the attack, the PCSP's IT department physically accesses the compromised ADSL modem/router equipment, performs a factory reset and reconfigures it to use new network credentials.

Attack Impact

The use case *Hijacking Access to National Healthcare Databases* directly impacts the primary care service provider's access to the national healthcare databases, causing a **loss of availability** of the associated service and information. The attack affects the **healthcare organisation** (the PCSP), as care delivery is hampered by the inability to access relevant information. The attack's expected recovery time is estimated to be **1 working day**, depending on the time required to identify the compromised equipment and to restore complete care service delivery.

SPHINX Role and Added-value Benefits

Dealing with the use case *Hijacking Access to National Healthcare Databases*, the SPHINX System is relevant in the early detection and identification of vulnerable critical assets (SPHINX vulnerability assessment), of the compromised equipment and of suspicious activity, including network scanning and password dictionary attacks (SPHINX anomaly detection, intrusion detection and security information and event management tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack and restoring the PCSP's access to the national healthcare databases (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Hijacking Access to National Healthcare Databases*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A PCSP accesses the national healthcare databases via the Internet, using a wireless ADSL modem/router. The ADSL equipment parameters (e.g., username, password, SSID, wireless key) remain unchanged from their factory default values.	SPHINX periodically conducts a vulnerability assessment the full IT infrastructure, including remote desktop applications and the ADSL modem/router equipment, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	The hacktivist uses a computer to scan the PCSP's network and recognises the ADSL equipment in use as one with known vulnerabilities.	SPHINX detects a network scanning activity coming from a previously unknown device. SPHINX generates an alert of the suspicious activity to warn the IT department.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Attack Phase	The hacktivist uses a brute force attack using known parameters (wireless key and default administrator password) to gain access to the administration interface of the modem/router equipment. The hacktivist changes the network access credentials, preventing the PCSP's medical staff to access the national healthcare databases and deliver adequate care.	SPHINX detects attempts to connect via a password dictionary attack to the network's ADSL router administrative interface. SPHINX issues an event notifying the IT department of the suspicious activity. SPHINX detects a successful login from an unauthorised device to the ADSL router administration interface. SPHINX elevates the event to incident and notifies the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures. For example, SPHINX suggests that the IT department blocks access and isolates the compromised device from the IT network.
Recovery Phase	The IT department needs to physically access the compromised equipment and reconfigure it to use new network credentials.	SPHINX collects relevant attack-related data, including compromised components (e.g., ADSL modem/router equipment), attack patterns, logs traffic data and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 9: SPHINX Role and Added-value Benefits in the Use Case Hijacking Access to National Healthcare Databases

4.3 UC3: Rootkit Malware Attack in a Cancer Treatment Institute

Use Case 3: Rootkit Malware Attack in a Cancer Treatment Institute	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Malicious action – Malware**
Threat Actor(s)	**Remote attackers – Cybercriminals**
Attack Vector(s)	**Interaction with users;** **Wired communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access**
Critical Healthcare Assets	
Affected Asset(s)	**Identification system;** **Healthcare data repositories;** **Healthcare data;** **IT and networking equipment**
Criticality of Affected Asset(s)	**Highly critical**

Table 10: Key Features of the Use Case Rootkit Malware Attack in a Cancer Treatment Institute

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case Description

A cybercriminal is recruited by a terrorist organisation to conduct a cyberattack that targets healthcare services, aiming to harm and cause fear to hundreds of patients, also affecting the citizens' perception of safety and security and compromising the trust in public healthcare services and in the Government.

The cybercriminal sends numerous emails carrying a new rootkit malware to different user recipients in the public cancer treatment institute. A negligent user from the institute's nursing staff opens the email, which infects the computer with a rootkit malware. Notwithstanding the title and body of the email being very convincing as if the email came from a safe sender, it is noted that users' negligence has increased due to working under pressure for long periods of time due to the conditions determined by the COVID-19 pandemic. And, although the computer is protected by antivirus/antimalware software, it does not detect the new type of rootkit malware that exhibits a very low profile (low CPU load and rarely uploads data) to avoid detection. Further, the new malware is able to circumvent the continuous monitoring of network devices against attacks by using evasion techniques. The cybercriminal slowly probes the existing firewall blocking network connections to detect holes and potential pivoting points, masks its remote IPs by using DNS side channels, effectively sidestepping the alerting mechanism in place. The sophisticated rootkit malware enables the cybercriminal to remotely monitor and control the infected computer, which is active 24 hours a day and shared by the medical and nursing staff to view patient data and prescribe medicine. It allows the cybercriminal to spy all the computer's activity for several months and, through keylogging, to steal the login credentials of several users, used to access the institute's healthcare information systems. Then, the cybercriminal utilises the stolen credentials to access those information systems, view the patients' medical data and alter the records (e.g., treatment plan and lab results).

Despite being well-trained to identify anomalies in patients' records, the medical and nursing staff is unable to prevent that, in a number of situations, patients receive the wrong treatment, causing their condition to deteriorate and their admission to intensive care units. As the number of these situations increases, so does the suspicion that the patient records are compromised. The medical and nursing staff make a formal incident report, informing the IT department of their suspicion.

Responding to the attack, the institute's IT department starts an investigation procedure: analysing the logs of several computers, the IT staff is able to identify the compromised computer and login credentials. Those accounts are immediately suspended, whereas the compromised computer receives a clean install. The patients' database is then restored from the latest backup prior to the attack.

Attack Impact

The use case *Rootkit Malware Attack in a Cancer Treatment Institute* directly impacts the cancer treatment institute's patient records, causing the **violation of the data integrity and confidentiality**. The attack affects not only the **healthcare organisation** (the cancer treatment institute) as care delivery can no longer rely on the accessible patient treatment plans, but also the **patients** who see their privacy violated. The attack's expected recovery time is estimated to be **several months**, depending on the time required to identify the exact altered patient data, to restore accurate patient records and to recover from the financial losses of supporting additional care to affected patients, of compensating the claims of affected patients and of implementing diverse promotional activities to recruit new patients and rebuild the institute's reputation.

SPHINX Role and Added-value Benefits

Dealing with the use case *Rootkit Malware Attack in a Cancer Treatment Institute*, the SPHINX System is relevant

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

in the identification of system vulnerabilities that allow the rootkit to be worm-able (SPHINX real-time cyber risk assessment tools), in the early detection of the attack by performing continuous monitoring of the network's and the database's activity (SPHINX data traffic monitoring, anomaly detection, intrusion detection and honeypot tools), in the prompt alerting of relevant IT staff of the suspicious network activity and database security breach (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack and restoring the institute's patient records (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Rootkit Malware Attack in a Cancer Treatment Institute*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	The cancer treatment institute provides diverse contact information, including email addresses, regarding the services they provide and the professionals supporting them.	SPHINX performs a cybersecurity verification, including a risk assessment to provide an estimation regarding the level of risks. SPHINX deploys a honeypot to serve as an early warning system for attacks and uses it to report the different ways the malware propagates inside the network. SPHINX reports to the IT department the results of the verification, ensuring that the IT department is aware of them and may take adequate protection measures.
Pre-Attack Phase	The cybercriminal selects as target the cancer treatment institute, as a healthcare organisation likely to generate significant impact in the general population and media coverage.	
Attack Phase	The cybercriminal sends several emails containing a rootkit malware that is executed when an email is opened. The infected computer occasionally accesses a remote website to upload collected data. The cybercriminal steals access credentials and is able to alter several patients' records. As a result, several patients receive the wrong treatment and their condition deteriorates.	SPHINX recognises the download of suspicious files that come in through email and suggests to the IT department to block the user's access to them. SPHINX recognises a suspicious external remote connection and recommends moving the computer providing the remote connection to a more restricted network environment for further inspection. The computer is denied access to the institute's network resources, namely the patients' databases, effectively countering the rootkit malware attack. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX allows the IT department to query the central logs repository at the security information and event management to identify if there are other machines that show the same or similar behaviours. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Recovery Phase	The IT department identifies the infected computer, suspends the compromised accounts and proceeds with a clean install of the computer. The patients' database is restored from the latest backup prior to the attack.	SPHINX collects relevant attack-related data, including information about the new rootkit malware used for the attack and traffic data logs including the destination IP addresses, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 11: SPHINX Role and Added-value Benefits in the Use Case Rootkit Malware Attack in a Cancer Treatment Institute

4.4 UC4: Theft of Health Data by Exploiting Vulnerable Software

Use Case 4: Theft of Health Data by Exploiting Vulnerable Software	
Scope	
Application Scenario	**eHealth Services**
Attack	
Threat Type	**Malicious action – Malware**
Threat Actor(s)	**Remote attackers – Opportunistic**
Attack Vector(s)	**Interaction with users;** **Wired communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Outdated system**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare information systems;** **Healthcare data**
Criticality of Affected Asset(s)	**Critical**

Table 12: Key Features of the Use Case Theft of Health Data by Exploiting Vulnerable Software

Use Case Description

An attacker uses the national portal for the public sector – whose access is open to the general public – and searches for procurement/purchases of IT software and equipment conducted by healthcare service providers over the last years, therefore identifying those that are most likely to own outdated IT software and equipment.

Within the list of vulnerable healthcare organisations, the attacker chooses a large health clinic that has acquired an inventory software that has not been updated with existing security patches and retrieves online the clinic's administrative email address that is likely to be vulnerable and identifies email address related with administrative departments via the hospital website.

The attacker sends several emails to the clinic impersonating a representative of a medical product supplier and providing an attached file looking like a PDF document (e.g., Invoice.pdf or Catalog.pdf) but delivering a JAVA Remote Access Trojan (RAT) malware specifically designed to exploit the known vulnerabilities of the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

clinic's inventory software.

An employee of the clinic's acquisition department tries to open the attached file, unaware that it is a JAVA executable. By doing so, the malware becomes active and infects the inventory software. It starts to log keystrokes (effectively stealing the user passwords), to retrieve sensitive files (contracts, employees' financial forms, logistic data) and to capture screenshots of the patients' medical records, uploading all collected information to a remote server controlled by the attacker. The attacker starts selling the information in the black market to interested buyers, including the clinic's suppliers and competitors.

The clinic's employees notice that the IT infrastructure is less responsive than usual and present claims to the IT department.

Acting on the claims, the IT department conducts an investigation and identifies the presence of the JAVA malware in the inventory software. They proceed with a clean installation of the inventory software, updated with the latest security patches, in all affected computers.

Attack Impact

The use case *Theft of Health Data by Exploiting Vulnerable Software* directly impacts the clinic's healthcare information systems, causing the **violation of data confidentiality** in what concerns the clinic's operations information, the employees' data and the patients' data. The attack affects the **healthcare organisation** (the clinic), as inventory/supply operations are halted and the access to the patients' databases suspended, thus causing significant delays in the administrative work, as well as the clinic's employees and patients who see their personal data exposed and sold online. The attack's expected recovery time is estimated to be **2 or 3 working days**, depending on the number of affected assets and on the effort required to re-install the updated inventory software. Still, **several months** may be required for the clinic to recover from the financial losses due to compensating claims by affected suppliers, employees and patients, and to marketing campaigns to procure new suppliers, recruit new employees and clients and rebuild the clinic's reputation.

SPHINX Role and Added-value Benefits

Dealing with the use case *Theft of Health Data by Exploiting Vulnerable Software*, the SPHINX System is relevant in the identification of unattended and vulnerable critical assets (SPHINX vulnerability assessment tool), in the early detection of the attack by performing continuous monitoring of the network's and the databases' activity (SPHINX data traffic monitoring, anomaly detection and security information and event management tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack and restoring the clinic's databases (SPHINX decision support tools).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Theft of Health Data by Exploiting Vulnerable Software*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	As per law, public purchases are openly accessible online. Individuals with malicious intent can use it to collect information about potential cyber vulnerabilities in public organisations. Healthcare organisations provide contact information, including email addresses.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including non-proprietary software and services used by proprietary software that is outdated and missing security patches, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	The attacker selects a clinic likely to have a vulnerable IT infrastructure.	
Attack Phase	The attacker sends several emails containing a malware executable disguised as a document file. The affected computers exhibit a high CPU load, access remote websites and upload a high amount of traffic.	SPHINX recognises the download of suspicious files coming in through email and suggests to the IT department to block the user's access to them. SPHINX recognises a suspicious external remote connection and recommends moving the affected computer to a controlled network environment to prevent the spreading of the RAT malware throughout the network and for further inspection. The computer is denied access to the clinic's network resources, namely the contracts, the employees and the patients' databases, effectively countering the RAT malware attack. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department needs to verify which computers were affected and proceed with a clean install for each of them.	SPHINX collects relevant attack-related data, including information about the infection method, which computers were compromised, which remote IP was used and traffic data logs and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 13: SPHINX Role and Added-value Benefits in the Use Case Theft of Health Data by Exploiting Vulnerable Software

4.5 UC5: Tampering with Medical Devices

Use Case 5: Tampering with Medical Devices	
Scope	
Application Scenario	**mHealth Services**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 5: Tampering with Medical Devices	
Attack	
Threat Type	**Malicious action – Medical device tampering**
Threat Actor(s)	**Insider threats**
Attack Vector(s)	**Interaction with users (social engineering);** **Wired communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Connected devices**
Critical Healthcare Assets	
Affected Asset(s)	**Networked medical devices**
Criticality of Affected Asset(s)	**Critical**

Table 14: Key Features of the Use Case Tampering with Medical Devices

Use Case Description

A device supplier aims to discredit its major competitors. The supplier is aware that medical devices are subjected to thorough testing procedures, followed by strict certification processes that are time and effort consuming. Thus, a stable configuration in their software and hardware components is required and, performing changes in either, requires repeating testing and, in some cases, even resubmitting the certification process. Consequently, the supplier foresees that competitors do not continuously update their medical devices with the latest security patches, meaning they are a vulnerability when connected to the hospital's network.

Planning to tamper with its competitors' medical devices, the device supplier finds a care centre employee that is extremely displeased with the management and approaches the employee, offering a financial reward for the execution of the attack. The plan is to release a virus using a USB stick that only targets specific medical devices from competitors.

Since the employee has physical access to several medical devices in the care centre, the attack is easily conducted, with the USB stick containing the virus being plugged to several medical devices, causing the worm activation and propagation throughout the network. In a matter of hours, the virus infected most of the medical devices at the care centre, causing malfunctions, continuous reboots and wrong measurements.

The nursing staff informs the care centre's management of the medical devices' erratic behaviour. The care centre's IT staff disconnects the medical devices and returns them for repair by the device manufacturers. When not covered by warranty, the care centre needs to pay for the repair costs. The care centre's management issues several formal complaints and terminates business relations with three devices suppliers, who endure a significant reputation loss. Until the devices are repaired, the care centre is limited in the quality of healthcare services it provides to its users.

Attack Impact

The use case *Tampering with Medical Devices* directly impacts the care centre's operations, causing a **loss of availability** of specific healthcare services and the **violation of the integrity of the users' data**, following the use of the infected medical devices. The attack affects the **healthcare organisation** (the care centre) and its **users**, as the care centre no longer provides specific healthcare services. Further, also the care centre's **medical device suppliers** are deeply affected by the attack, once the information is leaked and other customers demanded security assessments. The attack's expected recovery time is estimated to be **5 working days**,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

depending on the time spent to identify the infected medical devices and have them repaired, as well as on the effort required to reset the affected users' records.

SPHINX Role and Added-value Benefits

Dealing with the use case *Tampering with Medical Devices*, the SPHINX System is relevant in the cybersecurity certification of the medical devices and equipment (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the care centre), in the identification of vulnerable critical assets (SPHINX vulnerability assessment and real-time cyber risk assessment tool), in the early detection of attacks by identifying the compromised devices (SPHINX anomaly detection and honeypot tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack and the detection of the replication of virus events coming from multiple sources in quick succession (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Tampering with Medical Devices*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A medical device manufacturer aims to affect the credibility of its major competitors. Aware that manufacturers delay or do not incorporate security patches in medical devices in use, the device manufacturer founds a displeased care centre professional that is willing to help exploit the vulnerabilities of the medical devices when connected to the care centre's network.	SPHINX performs a thorough cybersecurity certification of the medical devices before they are connected to the network. Only when the medical devices receive SPHINX's approval for full security compliance, are they connected into the network. SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including connected medical devices, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures. SPHINX deploys a honeypot to detect the attack vectors and provide information on how to effectively detect the virus behaviour and its replication capabilities.
Pre-Attack Phase	The displeased employee is given the USB stick containing a virus to affect the medical devices.	
Attack Phase	The displeased employee has physical access to several medical devices and plugs the USB-stick with the virus to infect them. The virus propagates to several medical devices in the network and, within hours, they start to malfunction.	SPHINX detects suspicious network activity, caused by the virus propagation and identifies the source devices. SPHINX generates an alert of the suspicious activity to warn the IT department, recommending the transfer of the compromised devices to a restricted environment for further inspection. SPHINX identifies the presence and category of the virus and provides the IT department with a detailed report of the attack activity, identifying compromised assets

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
		and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department has to identify the infected medical devices, disconnect them from the network and send them for repair. In addition, the IT department proceeds with the reset of the user records affected by the wrong measurements collected from the infected medical devices.	SPHINX collects relevant attack-related data, including the device used for the attack and the compromised network components (e.g., medical devices and users' records) and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 15: SPHINX Role and Added-value Benefits in the Use Case Tampering with Medical Devices

4.6 UC6: Ransomware Attack to Healthcare Data

Use Case 6: Ransomware Attack to Healthcare Data	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Malicious action – Ransomware**
Threat Actor(s)	**Remote attackers – Organised crime**
Attack Vector(s)	**Interaction with users;** **Wired communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Shared network files (SMB protocol)**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare information systems;** **Healthcare data repositories;** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 16: Key Features of the Use Case Ransomware Attack to Healthcare Data

Use Case Description

A criminal organisation plans a large-scale ransomware attack targeting healthcare data, for it is a highly valuable asset and healthcare service providers are willing to pay so that their multi-million business is not disrupted.

Targeting a global healthcare service provider, with a large network of hospitals, clinics and laboratories, the cybercriminals develop a new sophisticated trojan – the Emotet malware – to infect file systems and lock access to infected computers. Unless the requested amount of money in virtual currency is paid to a specific account, the healthcare data of millions of patients will be forever lost, seriously compromising their healthcare treatment outcomes and quality of life.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

For a day, thousands of emails are sent to different hospitals, clinics and laboratories owned by a known worldwide healthcare service provider. In the emails, one attached file contains the Emotet malware in disguise and, once this file is opened by several users in the different facilities, the Trojan swiftly propagates throughout the healthcare service provider's network, exploiting known network share vulnerabilities and remaining undetectable by installed anti-virus programmes[3]. It is noted that users' negligence increased due to working under pressure for long periods of time due to the conditions determined by the COVID-19 pandemic. After working hours, the trojan initiates the encryption of the file systems across the organisation's hospitals, clinics and laboratories, effectively locking users from accessing the files. In a matter of hours, the healthcare service provider's databases are encrypted, including the healthcare records of thousands of millions of patients.

The healthcare service provider rapidly notices the presence and effects of the malware. At each facility, the IT department starts working hard to shut down the network, disconnect all computers and proceed with their reinstallation. The latest backups are used to restore the organisation's databases, although the amount of records lost depend on the backup policy of each hospital, clinic and laboratory. Meanwhile, the healthcare organisations have to revert to paper-based operations and cannot perform specific interventions requiring IT assets (e.g., diagnoses and database access).

Attack Impact

The use case *Ransomware Attack to Healthcare Data* directly impacts the healthcare service provider's operations, causing a **loss of availability** of healthcare databases, patient data and of healthcare services, namely those requiring IT-based systems. The attack affects the **healthcare organisation** (different hospitals, clinics and laboratories) and its **patients**, as they no longer are able to receive specific healthcare services. The attack's expected recovery time is estimated to be **1 or 2 months**, depending on the extent of the infection and on the time spent to reinstall the backup files to reset the encrypted data and to adopt secure protocols for file sharing across the different hospitals, clinics and laboratories.

SPHINX Role and Added-value Benefits

Dealing with the use case *Ransomware Attack to Healthcare Data*, the SPHINX System is relevant in the identification of vulnerable critical assets, including with respect to adopted network sharing protocols, such as the Server Message Block (SMB) protocols (SPHINX vulnerability assessment and real-time cyber risk assessment tools), in the early detection of attacks by identifying the compromised computers (SPHINX data traffic monitoring, anomaly detection, honeypot and security information and event management tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Ransomware Attack to Healthcare Data*.

[3] From mid-September to the early days of November 2020, Greek hospitals were attacked with the Emotet malware. Users consider the email looked legitimate and were comfortable with opening the attachment. Once they did, the malware affected their computer and spread. The SPHINX System would have been helpful to identify the email traffic and indicate the ICT departments to initialise mitigation actions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A criminal organisation plans a large-scale ransomware attack targeting the healthcare data hosted by a global healthcare service provider, with a large network of hospitals, clinics and laboratories.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including file server traffic protocols (e.g., SMBv1, SMBv2, SMBv3), and reports to the IT department the system's major vulnerabilities, ensuring that the professionals are aware of existing vulnerabilities to take adequate protection measures.
Pre-Attack Phase	The cybercriminals develop a new sophisticated malware to infect file systems and lock access to infected computers.	
Attack Phase	The cybercriminals send numerous emails to different hospitals, clinics and laboratories containing an infostealer malware in attached files. Once activated, the malware propagates through the computer network of hospitals, clinics and laboratories and begins to encrypt the system files, blocking the users' access.	SPHINX detects suspicious network activity caused by the malware propagation, identifies the source devices and identifies the presence and category of the malware. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX detects suspicious computer activity caused by the encryption of the file systems, namely high CPU load and high network activity. SPHINX generates an alert of the suspicious activity to warn the IT department. The alert identifies the computers originating the suspicious activity and SPHINX recommends that the IT department isolate those computers to prevent the spreading of the Trojan throughout the network and to enable further inspection. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures based on the information collected and provided by SPHINX Honeypot and Security Information and Event Management tools.
Recovery Phase	The IT departments of the hospitals, clinics and laboratories shut down the IT infrastructure, disconnect the computers and proceed with a clean install for each of them. In addition, new secure exchange protocols are adopted by the healthcare service provider.	SPHINX collects relevant attack-related data, including information about the infection method, which computers were compromised, which remote IP was used and traffic data logs and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 17: SPHINX Role and Added-value Benefits in the Use Case Ransomware Attack to Healthcare Data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4.7 UC7: Distributed Denial-of-Service Attack in Regional Hospital

Use Case 7: Distributed Denial-of-Service Attack in Regional Hospital	
Scope	
Application Scenario	**mHealth Services and Remote Patient Monitoring**
Attack	
Threat Type	**Malicious action – Distributed Denial-of-Service**
Threat Actor(s)	**Remote attackers – Opportunistic**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Web-based services**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare information systems; IT and networking equipment**
Criticality of Affected Asset(s)	**Critical**

Table 18: Key Features of the Use Case Distributed Denial-of-Service Attack in Regional Hospital

Use Case Description

To improve the quality of remote healthcare, a regional hospital decides to deploy an online accessible webserver that not only provides medical treatment guidelines to remote patients, but also enables the remote monitoring of patients using medical devices that connect via a VPN server to the hospital's IT systems.

An attacker with intention to extort money from the hospital, purchases a botnet capability in a dark web marketplace and uses it to initiate a distributed denial-of-service (DDoS) attack against the hospital's online portal and VPN server. The DDoS attack is initiated against the hospital's network infrastructure via a router, involving the *ping of death* and *mac-flooding* techniques. Under these circumstances, the hospital's network communications become slow, thus affecting the operation and availability of medical applications and leading to the total collapse of the hospital's IT infrastructure. The DDoS attack lasts for several days and, as a result, both mHealth and remote patient monitoring services are rendered non-operational during the period.

Because the hospital's IT department lacks the capability to continuously monitor the availability of online health services, the incident is only acknowledged a few days later as a result of several complaints raised by patients. The hospital is overflown with the contact attempts from remote patients that use the telephone and emails to contact their physicians and to reschedule telehealth appointments, thus disrupting the normal treatment process and the hospital's daily operations. In addition, since the remote patient monitoring was out of operation due to the lack of availability of the VPN, the data coming from the medical devices was not uploaded to the patients' records, which may have compromised the patients' health and wellbeing outcomes. As a result, the hospital is required to ask patients to come to an unscheduled appointment for follow-up, generating additional pressure in hospital's services.

The IT department starts to work in establishing a new VPN server to re-establish the remote patient monitoring service.

Attack Impact

The use case *Distributed Denial-of-Service Attack in Regional Hospital* directly impacts the hospital's operations,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

causing a **loss of availability** of the online portal and the mHealth and remote patient monitoring service. The attack affects the **healthcare organisation** (the regional hospital), which faces a total slowdown of all hospital applications and the collapse of the hospital's IT infrastructure, and its **patients**, as they no longer are able to receive specific mHealth services. The attack's expected recovery time is estimated to be **5 working days**, depending on the effort to re-establish the online portal and the mHealth and remote patient monitoring services. In the meantime, the hospital's staff is overwhelmed with the additional appointments to follow-up external patients.

SPHINX Role and Added-value Benefits

Dealing with the use case *Distributed Denial-of-Service Attack in Regional Hospital*, the SPHINX System is relevant in the identification of vulnerable critical assets, including online services (SPHINX vulnerability assessment tool), in the early detection of attacks by identifying the high volume of packets, bytes and connections per seconds (SPHINX data traffic monitoring and anomaly detection tools) as well as the compromised assets (SPHINX honeypot and intrusion detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement adequate recovery and mitigation procedures, including blocking the attack by suggesting to block the attacker's port based on network traffic information from the data traffic monitoring (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Distributed Denial-of-Service Attack in Regional Hospital*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A regional hospital decides to adopt online web services and remote patient monitoring using medical devices connected to the hospital via a VPN.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including the firewall CPU load and VPN connections (namely site-to-connections), and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures. SPHINX provides a Data Traffic Monitoring tool and an Anomaly Detection tool for real-time monitoring of high volume, high packets or connections per second. SPHINX also provides the Security Information and Event Management tool that logs all security-related information.
Pre-Attack Phase	The attacker purchases a botnet capability from a darknet marketplace.	
Attack Phase	The attacker performs a network scan to identify all the publicly exposed online web services and uses this information to initiate a DDoS attack against the	SPHINX continuously monitors the availability of the existing services and detects the lack of response of the honeypot exposed, mHealth service and remote patient monitoring service as a result of a DDoS attack.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
	hospital's online portal and VPN server, rendering non-operational the services providing treatment guidelines online and remote patient monitoring.	SPHINX generates an alert of the absence of activity to warn the IT department. Using the DoS attack patterns from the SPHINX Knowledge Base, SPHINX identifies the DDoS attack and provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department starts to work in establishing a new VPN server to re-establish the remote patient monitoring service.	SPHINX collects relevant attack-related data and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 19: SPHINX Role and Added-value Benefits in the Use Case Distributed Denial-of-Service Attack in Regional Hospital

4.8 UC8: Compromising Health Services through Cryptocurrency Mining

Use Case 8: Compromising Health Services through Cryptocurrency Mining	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Malicious action – Malware (cryptoworm)**
Threat Actor(s)	**Insider threat**
Attack Vector(s)	**Physical interaction with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment**
Criticality of Affected Asset(s)	**Critical**

Table 20: Key Features of the Use Case Compromising Health Services through Cryptocurrency Mining

Use Case Description

An IT employee of a medical laboratory has started to invest in cryptocurrency and is looking to generate revenues by mining it. Since cryptocurrency mining requires high computational resources and energy consumption, the IT employee decides to surreptitiously install the mining software in the laboratory's high-performing computers used by the technicians to perform the exams and diagnoses. Two advanced computers are setup to use external network ports and accept incoming connections, thus running the cryptocurrency mining programme.

Not being IT specialists, the laboratory team is disappointed at the slow response time of the state-of-the-art high-performance computers to process the exams and prepare the reports, causing a large delay in the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

completion of the reports and the issue of results. On its turn, this affects the laboratory's clients, including local hospitals and clinics, but also the patients that have their treatment plans affected by the delays in receiving their exam results, with significant impact in their health and quality of life.

Attack Impact

The use case *Compromising Health Services through Cryptocurrency Mining* directly impacts the medical laboratory's operations, causing a **loss of availability** of the laboratory exams and diagnoses reports in a timely manner. The attack affects the **healthcare organisation** (the medical laboratory) and its clients, including other **hospitals**, **clinics** and **patients**, as they no longer receive timely lab results and reports. The attack's expected recovery time is estimated to be **1 to 2 working days**, depending on the time to identify the compromised assets and to uninstall the cryptocurrency mining software.

SPHINX Role and Added-value Benefits

Dealing with the use case *Compromising Health Services through Cryptocurrency Mining*, the SPHINX System is relevant in the early detection of attacks by identifying the compromised assets (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Compromising Health Services through Cryptocurrency Mining*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	The medical laboratory uses high-performing computers that have access to several network ports and can accept incoming connections. The security policy in place allows the IT staff to freely install software.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures. SPHINX provides a Data Traffic Monitoring tool and an Anomaly Detection tool for real-time monitoring of high volume, high packets or connections per second.
Pre-Attack Phase		
Attack Phase	The IT employee installs unauthorised cryptocurrency mining software that consumes a high amount of resources, causing the advanced computers to be unresponsive to their day-to-day tasks, significantly delaying operations related	SPHINX continuously monitors resource metrics and the availability of the existing services to detect lack of response of nominal services on critical computers, as a result of the deviation of resources to cryptocurrency mining activities. SPHINX generates an alert of the absence of activity in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
	with lab results and reports.	specific computers to warn the IT department. SPHINX identifies the cryptocurrency mining software and provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department performs the uninstallation of the cryptocurrency mining software to recover all available resources to perform healthcare related activity.	SPHINX collects relevant attack-related data and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 21: SPHINX Role and Added-value Benefits in the Use Case Compromising Health Services through Cryptocurrency Mining

4.9 UC9: Compromised BYOD Enables Stealing of Patient Data

Use Case 9: Compromised BYOD Enables Stealing of Patient Data	
Scope	
Application Scenario	**mHealth Services**
Attack	
Threat Type	**Malicious – Malware**
Threat Actor(s)	**Remote attackers – Cybercriminals**
Attack Vector(s)	**Human Error – Non-compliance to security procedures**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Non-compliance to security procedures**
Critical Healthcare Assets	
Affected Asset(s)	**Identification system;** **Mobile user devices;** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 22: Key Features of the Use Case Compromised BYOD Enables Stealing of Patient Data

Use Case Description

To expedite healthcare service delivery, a clinic adopted mHealth services and provides its medical and nursing staff with mobile devices (tablets) to facilitate the execution of specific care activities. These devices run an outdated operating system and have no antivirus programme; thus, they have connection to the clinic's wireless network but not to the Internet.

While using its tablet, a doctor wants to navigate the Internet. Bypassing the clinic's security policy, the doctor uses the hotspot function in the smartphone to connect the tablet to the Internet. While navigating the Internet, the doctor clicks on an advertisement unaware that it runs a malicious code exploiting zero days on

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

the tablet browser and using that hole to install malware into the tablet. The malware is designed to store keylogging data, screen touch locations and screenshots in the tablet's local file space and then to transmit the stored data to the attacker's online server each time the doctor reconnects the tablet to the Internet using the smartphone. In the process, the attacker is able to collect sensitive information related with the clinic, including patients' records the doctor consulted and the doctor credentials. The attacker contacts the clinic by email, using an anonymous account, and presents samples of the stolen data, including the sensitive patient information, demanding payment not to expose this information to the Internet, negatively affecting the clinic's reputation and the trust of the patients.

As soon as the IT department is informed of the attack, the IT staff proceeds to identify the compromised assets and then proceeds with a clean installation of the tablet. New access credentials are also created for the doctor.

Attack Impact

The use case *Compromised BYOD Enables Stealing of Patient Data* directly impacts the clinic's operations, causing the **violation of confidentiality** of the patients' sensitive data. The attack affects the **healthcare organisation** (the clinic), as well as the clinic's **patients** who have their personal data exposed. The attack's expected recovery time is estimated to be **1 working day**, in order to identify the affected assets, clean the malware in the tablet and generate new access credentials for the doctor. Still, if the attacker proceeds to sell online the patient data, **several months** may be required for the clinic to rebuild its reputation and recover from the financial losses due to compensating claims by affected patients.

SPHINX Role and Added-value Benefits

Dealing with the use case *Compromised BYOD Enables Stealing of Patient Data*, the SPHINX System is relevant in the identification of outdated and vulnerable critical assets (SPHINX vulnerability assessment tool), in the early detection of the attack by performing continuous monitoring of the network's activity (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement adequate recovery and mitigation procedures, including blocking the attack and restoring the clinic's databases (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Compromised BYOD Enables Stealing of Patient Data*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	Adopting mHealth services, the clinic uses tablets that are outdated and lack anti-virus software. These tablets are only connected to the clinic's network and have no Internet access.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including connected devices and software that is outdated and missing security patches, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attac k	The doctor overcomes the clinic's security policy by creating a WiFi	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
	hotspot using his mobile phone to access the Internet. A malware is installed in the tablet when the doctor clicks on an advertisement.	
Attack Phase	A malware is installed in the tablet when the doctor clicks on an advertisement. The malware collects information about the doctor credentials and patient records. Whenever the tablet is connected to the Internet, the malware uploads the collected information to the attacker's online server. The attacker contacts the clinic, demanding payment not to disclose the patient information.	SPHINX monitors and logs network connection, namely concerning online resources, for all connected devices. SPHINX recognises a suspicious external remote connection and generates an alert of the suspicious activity to warn the IT department. The IT department transfers the computer providing the remote connection to an isolated network environment for further inspection. The computer is denied access to the clinic's resources, namely the patients' databases. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department identifies the compromised assets and proceeds with a clean installation of the tablet. It also issues new credentials for the doctor.	SPHINX collects relevant attack-related data, including information about the infection method, which computers were compromised, which remote IP was used and traffic data logs and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 23: SPHINX Role and Added-value Benefits in the Use Case Compromised BYOD Enables Stealing of Patient Data

4.10 UC10: Taking Control of Connected Medical Devices

Use Case 10: Taking Control of Connected Medical Devices	
Scope	
Application Scenario	**mHealth Services**
Attack	
Threat Type	**Malicious action – Medical device tampering**
Threat Actor(s)	**Remote attackers – Government-sponsored**
Attack Vector(s)	**Interaction with users (social engineering);** **Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Connected devices**
Critical Healthcare Assets	
Affected Asset(s)	**Networked medical devices;** **Healthcare data**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 10: Taking Control of Connected Medical Devices	
Criticality of Affected Asset(s)	**Highly critical**

Table 24: Key Features of the Use Case Taking Control of Connected Medical Devices

Use Case Description

A rogue government is targeting a high-profile public figure that is receiving treatment at a hospital. The government contracts a cybercriminal to explore the hospital's vulnerabilities, collect sensitive data about the high-profile patient and, if possible, disrupt the associated treatment plan.

The cybercriminal starts by scanning the hospital's external network, looking for a hole to pivot in. Several state nation attack tools are employed and they identify an asset as having a SQL injection vulnerability. The cybercriminal successfully exploits it and is able to get a remote shell from which the cybercriminal performs a slow recognisance to locate connected medical devices. The cybercriminal analyses the hospital's IT network and connected medical equipment, identifying several devices presenting known vulnerabilities (e.g., MRI scanners, CT scanners, blood chemistry analysers). Analysing the technical specifications of a vulnerable blood chemistry analyser, freely available in the manufacturer's site, the cybercriminal identifies known vulnerabilities in their network and interface protocols.

After identifying the medical device to exploit, the cybercriminal poses as a maintenance technician of the blood chemistry analyser manufacturer and uses social engineering techniques to persuade the hospital staff to grant remote access to the blood chemistry analyser. In possession of this access, the cybercriminal is then able to access the blood analyser's interface protocols and through them, enter the patients' databases, retrieving sensitive medical data, including the one pertaining to the high-profile public figure. Specifically, the analysis confirms the presence of illicit drugs in the public figure's bloodwork, information that, if made public, could ruin the public figure's career. Furthermore, as instructed, the cybercriminal alters the report on the blood test results, causing a disruptive change in the public figure's treatment plan.

Because a single patient has been targeted, this attack is likely to remain undetectable by IT security resources. Days or weeks may unfold before the equipment-induced error is identified and corrected. And even when noticed, it can easily by attributed to a fault in the medical device and not to a malicious external action. Importantly, the recovery of this attack requires the collaboration between the hospital and the device manufacturer.

Attack Impact

The use case *Taking Control of Connected Medical Devices* directly impacts the clinic's operations, causing the **violation of integrity and confidentiality** of the patient's sensitive data. The attack affects the **healthcare organisation** (the hospital), as well as the **patient** whose personal data is stolen and whose treatment plan is affected, compromising health and wellbeing outcomes. The attack's expected recovery time is estimated to be **1 working day**, in order to identify the affected asset and reconfigure the device before connecting it to the hospital's network. Still, the harm done to the high-profile public figure is irreparable.

SPHINX Role and Added-value Benefits

Dealing with the use case *Taking Control of Connected Medical Devices*, the SPHINX System is relevant in the cybersecurity certification of medical devices and equipment (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the hospital), in the identification of vulnerable critical assets

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

(SPHINX vulnerability assessment tool), in the early detection of the attack by performing continuous monitoring of the network's activity (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the collection and storage of logs from the multiple connected devices to enable adequate investigation (SPHINX security information and event management), in the presentation of a detailed report on the cyberattack (SPHINX forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack and restoring the clinic's databases (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Taking Control of Connected Medical Devices*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A rogue government targets a high-profile public figure that is receiving treatment at a hospital. They contract a cybercriminal to explore the hospital's vulnerabilities, collect sensitive data about the high-profile patient and, if possible, disrupt the associated treatment plan.	
Pre-Attack Phase	The cybercriminal analyses the hospital's IT network and identifies vulnerable connected medical devices, including a blood chemistry analyser, whose technical specification, available in the manufacturer's site, allow for the identification of the network and interface protocols used to access patient records and to remotely update the device's configuration (e.g., change the dosage level of a substance).	SPHINX performs a thorough cybersecurity certification of the medical devices before allowing them access to the network. Only when medical devices receive the SPHINX approval for full security compliance, are they connected into the network. SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Attack Phase	The cybercriminal uses social engineering techniques to persuade the hospital staff to provide access to the medical device via a remote connection (e.g., AnyDesk or TeamViewer). Once the access is granted, the cybercriminal accesses the analyser's configuration as well as the hospital's patient records, namely those pertaining to the high-profile public figure. The cybercriminal downloads the patient data and proceeds to alter the analyser's test results, disrupting the public figure's treatment plan.	SPHINC detects a network scanning activity and issues an alert to the IT staff. SPHINX detects a suspicious external remote connection and the attempt to access the medical device records and identifies the source device. SPHINX generates an alert to warn the IT department and recommends the transfer of the affected assets to an isolated network environment for further inspection. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Recovery Phase	The IT department identifies the compromised medical device that is delivering wrong diagnoses, disconnect it from the network and contacts the device manufacturer for adequate repair. In collaboration with the manufacturer, the IT department learns that the equipment malfunction was indeed caused by a malicious attack.	SPHINX collects relevant attack-related data, including the device used for the attack and the compromised patient records and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 25: SPHINX Role and Added-value Benefits in the Use Case Taking Control of Connected Medical Devices

4.11 UC11: Intrusion in the Clinical Centre's Wireless Network

Use Case 11: Intrusion in the Clinical Centre's Wireless Network	
Scope	
Application Scenario	**mHealth Services**
Attack	
Threat Type	**Malicious action – Hijacking**
Threat Actor(s)	**Malicious external user**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Wireless connectivity;** **Unattended legacy systems**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment**
Criticality of Affected Asset(s)	**Critical**

Table 26: Key Features of the Use Case Intrusion in the Clinical Centre's Wireless Network

Use Case Description

As part of its mHealth services policy, a clinical centre provides a WiFi network allowing its clerical and clinical staff to easily access the centre's IT resources, namely the healthcare information systems and the healthcare databases. The centre's WiFi network uses WPA2 protection with 256-bit encryption key; however, it openly broadcasts its SSID and the password set is very weak, based on a simple dictionary word ("password"). Moreover, the IT department did not change the router's default configuration access credentials (user "admin" and password "admin").

A visiting guest to the centre detects the existing WiFi network and, using a simple WiFi cracker and a dictionary file, manages to crack the password. The attacker guest is then able to access the router administration console and change its configuration. While performing a network scan, the attacker guest identifies several switches that, having reached end-of-life, are not patched by the manufacturer and display known vulnerabilities. The attacker is also successful in connecting to those switches and alter their configuration. As a result of this attack, the clinical centre's wired and WiFi network is disabled and the centre's IT resources are no longer accessible

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

to the centre's clerical and clinical staff, seriously compromising the healthcare service delivery.

Once the breach is detected, the IT department proceeds with the reconfiguration of the networking devices, performing a factory reset in the WiFi router and implementing stronger passwords, including for all connected WiFi assets used by the centre's staff.

Attack Impact

The use case *Intrusion in the Clinical Centre's Wireless Network* directly impacts the clinical centre's operations, causing the **loss of availability** of all healthcare services that are IT-dependent and forcing the centre's staff to revert to paper-based operations, where possible. The attack hinders the **healthcare organisation** (the clinical centre), affecting its capability to provide healthcare services and seriously threatening the health and wellbeing of its patients. The attack's expected recovery time is estimated to be **1 working day**, in order to identify affected assets and reconfigure the networking devices before enabling access to the centre's databases.

SPHINX Role and Added-value Benefits

Dealing with the use case *Intrusion in the Clinical Centre's Wireless Network*, the SPHINX System is relevant in the identification of vulnerable critical assets (SPHINX vulnerability assessment tool), in the early detection of the attack by performing continuous monitoring of the network's activity (SPHINX honeypot, anomaly detection, security information and event management, intrusion detection and data traffic monitoring tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Intrusion in the Clinical Centre's Wireless Network*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	The WPA2 password used in the clinical centre's WiFi wireless network is weak and the WiFi router admin console uses the factory password.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including connected networking equipment and observation of complex password policies, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	A guest at the clinical centre scans the centre's wireless network and runs a WiFi password cracker tool in order to access the router.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Attack Phase	The attacker guest manages to crack the WPA2 password, thus gaining access to the clinical centre's network. Then, he scans all network devices and discovers several switches with known vulnerabilities and manages to connect to them and alter their configuration. As a result, the clinical centre's clerical and clinical staff is no longer able to access the centre's wired and WiFi network and its IT resources.	SPHINX detects a password brute force attempt to access the clinical centre's WiFi router, identifies the source device's MAC address and recommends blocking its access. SPHINX detects the unauthorised network scan activities within the emulated IT system, identifying the source machine. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department physically accesses the compromised networking devices (routers, switches) to perform a factory reset. In addition, all networking devices are reconfigured to use new network credentials.	SPHINX collects relevant attack-related data, including the about the computer used for the attack, the compromised network devices and the used remote IP address, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 27: SPHINX Role and Added-value Benefits in the Use Case Intrusion in the Clinical Centre's Wireless Network

4.12 UC12: Hacking Health IT Systems

Use Case 12: Hacking Health IT Systems	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Human error – Non-compliance to security procedures**
Threat Actor(s)	**Malicious external users – Opportunistic**
Attack Vector(s)	**Interaction with users (social engineering);** **Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Non-compliance to security procedures**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment;** **Healthcare information systems**
Criticality of Affected Asset(s)	**Highly critical**

Table 28: Key Features of the Use Case Hacking Health IT Systems

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case Description

A rehabilitation care unit does not have specialised cybersecurity skills in its IT department. In that unit, a young patient has been receiving intensive treatment for several months and develops a good relationship with the care staff. Because the care unit does not provide guest Internet access, the young patient convinces the care staff to provide the password of the unit's private wireless network. Inadvertently, the carer delivers to the young patient the access to the care unit's IT resources and databases, including the patient records.

The young patient has good cyber-security know-how and expertise and sees the access to the care unit's IT resources as a good opportunity to exercise her white-hacking skills. Accessing the care unit's wireless network using network scanning, the young patient is able to build a map of the network connected devices, extracting detailed information concerning used operating systems, browsers and network protocols. The white-hacker also deploys packet sniffers that, as a result of the system not using encrypted communications, is able to collect user credentials and identifies the location of sensitive information, including financial information, contracts, employee personal information and medical data.

The young patient's intent is to draft a detailed report, informing the care unit of their IT vulnerabilities. The white hacker drafts the report, adding sufficient evidence to support the findings and proposing relevant security measures to improve cybersecurity policies and practice in the care unit. The report provides actionable intelligence to the care unit's management that decides to upgrade its cybersecurity system, using the young patient's skilled advice.

Attack Impact

The use case *Hacking Health IT Systems* portrays the activity of a white hacker. Should the same situation have been exploited by a malicious actor, it would have directly impacted the care unit's operations, causing the **loss of availability** of all healthcare services that are IT-dependent and forcing the care unit's staff to revert to paper-based operations, where possible. In addition, it would have impacted **the integrity and the confidentiality of the patient data** hosted by care unit's healthcare repositories and databases. The attack affects the **healthcare organisation** (the care unit), affecting its capability to provide healthcare services and seriously threatening the health and wellbeing of its patients.

SPHINX Role and Added-value Benefits

Dealing with the use case *Hacking Health IT Systems*, the SPHINX System is relevant in the identification of vulnerable assets with default or weak credentials (SPHINX vulnerability assessment tool), in the early detection of the attack by performing continuous monitoring of the network's activity (SPHINX honeypot, anomaly detection, intrusion detection and data traffic monitoring tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Hacking Health IT Systems*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	The rehabilitation care unit lacks cyber-security skills. The security policies adopted are weak, the IT network has several vulnerabilities and the staff has no cyber-security training awareness.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, maintaining a database of the network MAC addresses and a log from switches and firewalls, as well as the use of non-encrypted communications between systems and a list of weak passwords and default credentials, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	The rehabilitation care unit has been providing intensive treatment to a young patient for several months and good relations have been established. The care staff give the young patient the password of the unit's private wireless network.	
Attack Phase	The young patient connects the computer to the hospital network. The patient runs a network scan to build awareness of the care unit's IT resources, existing vulnerabilities and, using a packet sniffer, retrieves several user credentials that give access to the care unit's healthcare databases.	SPHINX detects the use of non-encrypted communications between systems, a new unauthorised device trying to enter the care unit's network, suspicious network activity caused by the network scanning and a brute-force password attack. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department receive a vulnerability report provided by the young patients, helping them to implement better cybersecurity policies.	SPHINX collects relevant attack-related data, including source and attack method, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 29: SPHINX Role and Added-value Benefits in the Use Case Hacking Health IT Systems

4.13 UC13: Exploiting Remote Patient Monitoring Services

Use Case 13: Exploiting Remote Patient Monitoring Services	
Scope	
Application Scenario	**mHealth and Remote Patient Monitoring Platforms**
Attack	
Threat Type	**Malicious action – Malware**
Threat Actor(s)	**Remote Attackers - Opportunistic**
Attack Vector(s)	**Wireless communication with IT assets**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 13: Exploiting Remote Patient Monitoring Services	
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Poor cyber security practices**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 30: Key Features of the Use Case Exploiting Remote Patient Monitoring Services

Use Case Description

A patient undergoes a cardiac intervention (coronary angioplasty) and, six hours after the surgery, the patient is discharged from the hospital and admitted to the remote patient monitoring service, by which a set of medical equipment and devices and the telehealth service are assigned to continuously monitor the patient's recovery and care, in a home environment.

The patient uses a mobile App to read the vital signs data captured by the medical devices. Via the home WiFi router, the App connects to the Internet and uploads the vital signs data to the hospital's remote patient monitoring platform. The medical cardiology team accompanying the patient has then the actionable intelligence to timely act in case any vital signs lie outside threshold parameters. The patient monitoring platform implements secure user authentication mechanisms, but the patient vital signs data is not sent encrypted.

The patient's home network is protected by a weak password that is easily cracked by an opportunist hacker that is able to access the Internet router equipment and infect it, using the VPNFilter malware. This malware has been instructed to monitor all web traffic and, by forcing communications to non-transport layer security (TLS) mode[4], to capture any healthcare-related information and to modify its assigned data results. Hence, the patient's vital signs data received at the hospital's remote patient monitoring platform are different from the ones uploaded by the patient through the remote patient monitoring service.

As a result of this attack, the medical cardiology team following the patient receives an alert that the patient is in critical condition. The emergency service is notified to send immediately an ambulance for the patient, so that he may be re-admitted to the hospital and new exams be performed in order to explain the patient's status.

Only when the new exams' results do not support the diagnosis inferred from the patient data received by the hospital's remote patient monitoring platform, does the patient use the App to clarify the medical team on the exact results monitored by the remote patient monitoring platform. Rapidly it is detected a mismatch of the patient data and a warning is issued to the hospital's IT department.

The hospital's IT department performs a data integrity check, identifying that the data has being tampered with.

Attack Impact

The use case *Exploiting Remote Patient Monitoring Services* directly impacts the hospital's quality of service, causing the **loss of data integrity** of the patient data being transferred through the mHealth and remote patient monitoring service. The attack affects the **healthcare organisation** (the hospital), affecting the delivery of the

[4] This attack vector exploits potential security vulnerabilities where HTTPS is not available (HTTPS service is denied by the malware) and software accepts plain HTTP connections.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

mHealth and remote patient monitoring service and determining the activation of costly alternative healthcare services (unnecessary re-admission, additional exams, medical emergency transportation) to handle adequate healthcare delivery. In addition, this attack not only undermines the healthcare organisation's trust in the supplier of the remote patient monitoring platform but also weakens the patient's trust in the services provided by the healthcare organisation, possibly impacting negatively on the patient's recovery and health outcomes.

SPHINX Role and Added-value Benefits

Dealing with the use case *Exploiting Remote Patient Monitoring Services*, the SPHINX System is relevant in the identification of unattended and vulnerable critical assets (SPHINX vulnerability assessment and real-time cyber risk assessment tools), in the early detection of the attack by performing continuous monitoring of the web traffic activity (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool). Moreover, the detailed cybersecurity report generated by SPHINX also supports the supplier of the remote patient monitoring platform in performing the required security fixes.

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Exploiting Remote Patient Monitoring Services*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A patient is admitted to the remote patient monitoring service in a home environment. The patient uses the Internet and a mobile App to upload vital signs data to the hospital's remote patient monitoring platform.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure and monitors the use of non-encrypted communications, reporting to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	The patient's home network is protected by a weak password that is cracked by an opportunist hacker. The attacker is able to access the Internet router equipment.	
Attack Phase	The attacker infects the patient's home router using the VPNFilter malware, which is instructed capture and modify healthcare-related information. The medical cardiology team are alerted, requesting the patient to be readmitted to hospital care.	SPHINX continuously monitors the network, identifying the absence of encrypted end-to-end communication. SPHINX issues an alert to the IT department, identifying the attack source (herein external to the hospital, assigned to a known patient) and affected assets (specifically, the server hosting the remote monitoring service). Subsequently, the hospital staff is able to promptly contact the patient and check the patient's condition. SPHINX provides the IT department with a detailed report of the attack activity, identifying potential compromised assets and suggesting proper course of action for recovery and mitigation measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Recovery Phase	It is detected a mismatch of the patient data between what is registered in the patient's App and what is received at the hospital. The hospital's IT department confirms that the patient data has being tampered with.	SPHINX collects relevant attack-related data, including source and attack method, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences. The hospital's supplier of the Remote Monitoring Service is informed of the security vulnerability in its product and, using the SPHINX cybersecurity report, is able to promptly fix them.

Table 31: SPHINX Role and Added-value Benefits in the Use Case Exploiting Remote Patient Monitoring Services

4.14 UC14: Zero Day Attack to eHealth Services

Use Case 14: Zero Day Attack to eHealth Services	
Scope	
Application Scenario	**eHealth Services**
Attack	
Threat Type	**Malicious action – Malware**
Threat Actor(s)	**Remote Attackers – Cybercriminals**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Unknown vulnerability**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare information systems;** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 32: Key Features of the Use Case Zero Day Attack to eHealth Services

Use Case Description

A well-known chain of hospitals, clinics and medical centres announces the adoption of a new Laboratory Information System (LIS) to manage all patient lab analysis, exams and diagnostic reports, as part of the eHealth Services made available online by the Medical Group. They report that the LIS is a new software development adapted to the specific needs of the Medical Group, a significant investment that will allow the medical staff from the different medical units in the Group, as well as the patients, online access to the patient data.

Upon this news announcement, a known cybercriminal group holds a competition to access the new LIS software and search through the LIS code, looking for vulnerabilities. One of the cybercriminals is skilled enough to find an unknown vulnerability in the software and creates a dedicated exploit code that allows planting a malware in the LIS and steal patient data from the Medical Group's different hospitals, clinics and medical centres. The cybercriminal then proposes to share the unknown vulnerability details with the software vendor and return all patient data to the Medical Group for a substantial sum to be paid in bitcoins. Since the zero-day attack happened once the software vulnerability was identified, the LIS software vendor had no opportunity to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

create a patch to fix the vulnerability and is therefore willing to pay for the information that will allow the new LIS software to be no longer compromised.

Attack Impact

The use case *Zero Day Attack to eHealth Services* directly impacts the Medical Group's operations, causing the **violation of integrity and confidentiality** of the patient's sensitive data. The attack affects several **healthcare organisations** (the Group's hospitals, clinics and medical centres), as well as the patients whose personal data is stolen and whose treatment plan is affected, compromising their health and wellbeing outcomes. In addition, there is a significant negative impact on the LIS software vendor that not only sees its reputation severely affected but also has to pay for the information on the exploited vulnerability in its new software. The attack's expected recovery time is estimated to be **3 working days**, in order to isolate the affected software from the Medical Group's network and reconfigure the network to the old laboratory information system. Patients are scheduled for new exams and lab works but the harm done to the Medical Group's name and reputation is irreparable.

SPHINX Role and Added-value Benefits

Dealing with the use case *Zero Day Attack to eHealth Services*, the SPHINX System is relevant in the identification of vulnerable critical network entities and assets (SPHINX vulnerability assessment and real-time cyber risk assessment tools), in the early detection of the attack by detecting intrusion attempts (SPHINX data traffic monitoring, anomaly detection and intrusion detection tools) and identifying the compromised asset (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack and restoring the hospital's IT infrastructure (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Zero Day Attack to eHealth Services*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A new LIS software comes online to support a Medical Group's eHealth services offer.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures. The SPHINX Real-time Cyber Risk Assessment tool provides a space (security protocol analysis mechanisms) for testing protocols, allowing the IT department to update the list of known vulnerabilities with new ones. The SPHINX Honeypot serves as an early warning system for attacks, reporting the different ways the malware is trying to propagate inside the network.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

		The SPHINX Data Traffic Monitoring and Anomaly Detection tools enable the real-time monitoring of high volume, high packets or connections per second. These tools monitor the network traffic for common attack patterns, based on information provided by the SPHINX Knowledge Base.
Pre-Attack Phase	A cybercriminal group holds a competition to access the new LIS software and search through the LIS code, looking for vulnerabilities. One of the cybercriminals is skilled enough to find a hole in the LIS software.	
Attack Phase	The cybercriminal creates a dedicated exploit code that allows planting a malware in the LIS and steal patient data from the Medical Group's different hospitals, clinics and medical centres. The cybercriminal proposes to share the vulnerability details with the software vendor and return all patient data to the Medical Group for a substantial amount of money.	SPHINX continuously monitors the network, detects anomalous behaviour, including network scanning activities and intrusion attempts, and identifies the malware originating in the new LIS software. SPHINX generates an alert whenever suspicious and anomalous behaviour is detected to warn the IT department. SHPINX continuously updates a local knowledge base of new vulnerabilities and attack patterns. Based on this knowledge base, internal services can enforce mitigation or protection policies. SPHINX provides the IT departments with detailed reports of the zero-day attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The Medical Group's IT departments identify the LIS software and proceed with the installation of the old LIS software. Patients are scheduled for new exams and lab works. The LIS software vendor contacts the cybercriminals to pay for information on the LIS vulnerability.	After an attack incident, SPHINX collects all gathered data and propagates them to the appropriate services for processing. This will generate new attack pattern data that will update the system's knowledge base. SPHINX collects relevant attack-related data, including source and attack method, and delivers to the IT departments detailed reports of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 33: SPHINX Role and Added-value Benefits in the Use Case Zero Day Attack to eHealth Services

4.15 UC15: Theft of Hospital Equipment

Use Case 15: Theft of Hospital Equipment	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Malicious actions – Social Engineering**
Threat Actor(s)	**Insider threats**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 15: Theft of Hospital Equipment	
Attack Vector(s)	**Interaction with users;** **Physical interaction with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access;** **Non-compliance to security procedures**
Critical Healthcare Assets	
Affected Asset(s)	**Mobile user devices;** **Healthcare information systems**
Criticality of Affected Asset(s)	**Highly critical**

Table 34: Key Features of the Use Case Theft of Hospital Equipment

Use Case Description

In a hospital's psychiatric ward, a patient with strong IT knowledge is receiving treatment for a long period of time. During this time, the patient develops a good relationship with the ward's nursing staff and because the patient is deemed not threatening, there is leniency on the nursing staff's part that allow the patient to have access to the ward's nursing post and reception. Here-in, the patient has access to the nurse's computers, tablets and mobile phones. One day, the patient is able to steal an old mobile phone belonging to the ward that still has stored login credentials allowing anyone using the device to connect to the hospital's information systems, including the building management system.

The patient accesses patient treatment plans and changes the prescribed medication and dietary restrictions to all psychiatric patients in the ward. Further, the patient accesses the building management system (BMS) and alters the settings of the room temperature in the psychiatric ward.

The hospital's IT department identifies the stolen equipment that has accessed and changed patient data and room temperature controls. The device is located in the patient's room and, once retrieved, a factory-reset is performed. The hospital's patient data that has been tampered with (medication and diets of psychiatric patients) is changed back to the last valid settings. Likewise, the IT staff restores the hospital's BMS to the last valid configuration.

Attack Impact

The use case *Theft of Hospital Equipment* directly affects the hospital's operations, affecting the ward's controlled ambient and meals and causing the **violation of the integrity and confidentiality** of the patients' sensitive data. The attack affects the **healthcare organisation** (the hospital), as well as the **patients** whose personal data is breached and whose treatment plans are affected, compromising health and wellbeing outcomes. The attack's expected recovery time is estimated to be **1 working day**, in order to identify the stolen asset and reset it before connecting it to the hospital's network, as well as to restore the patient data and the BMS controls to the last valid settings.

SPHINX Role and Added-value Benefits

Dealing with the use case *Theft of Hospital Equipment*, the SPHINX System is relevant in the identification of obsolete and vulnerable critical assets (SPHINX vulnerability assessment tool), in the early detection of the attack by identifying the stolen asset and unauthorised access to network resources (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack and restoring the hospital's IT infrastructure (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Theft of Hospital Equipment*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A patient in the psychiatric ward develops a good relationship with the nursing staff and is allowed to have access to the ward's nursing post and reception, where nurse's computers, tablets and mobile phones may be found.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including connected hospital equipment, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures. SPHINX maintains a database of the mac addresses connected to the network, facilitating their discovery and monitoring. SPHINX also keeps a record of all stolen equipment.
Pre-Attack Phase	The patient steals an old mobile phone belonging to the ward that still has stored login credentials allowing anyone using the device to connect to the hospital's information systems.	
Attack Phase	The patient accesses the patient treatment plans and changes the prescribed medication and dietary restrictions to all psychiatric patients in the ward. Further, the patient accesses the hospital's building management system (BMS) and alters the settings of the room temperature in the psychiatric ward.	SPHINX continuously monitors the network and alerts the IT department about the operation of an equipment after a long period of absence or about the stealing of equipment. SPHINX detects suspicious network activity, identifies the source device and generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying the compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The hospital's IT department identifies the stolen equipment that accessed and changed patient data and room temperature controls. The device is located in the patient's room and retrieved to be factory-reset. The hospital's patient data that has been tampered with (medication and diet of psychiatric patients) is changed back to the last valid settings. The same process is performed in the BMS configuration.	SPHINX collects relevant attack-related data, including information about the intrusion method, the compromised equipment and traffic data logs and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 35: SPHINX Role and Added-value Benefits in the Use Case Theft of Hospital Equipment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4.16 UC16: Intercepting Cross-border Healthcare Data Exchange

Use Case 16: Intercepting Cross-border Healthcare Data Exchange	
Scope	
Application Scenario	**Cross-border Healthcare Service Delivery**
Attack	
Threat Type	**Malicious actions – Man-in-the-middle attack;** **Human error – Non-compliance to security procedures**
Threat Actor(s)	**Remote attacker – Opportunistic**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Unsecure protocols (HTTP and email);** **Non-authenticated access to IT infrastructure**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare data**
Criticality of Affected Asset(s)	**Critical**

Table 36: Key Features of the Use Case Intercepting Cross-border Healthcare Data Exchange

Use Case Description

A Swedish tourist in Malta is suddenly taken ill and seeks for emergency medical assistance in a Maltese outpatient surgical facility. As the tourist is consulted by the medical staff, the attending doctor has a number of questions about the patient's health condition and history and asks for access to the patient's medical data (computerised tomography or CT exams and records stored in the Swedish healthcare system). Once the patient provides the Maltese doctor the contacts of the doctor in Sweden, the Maltese doctor sends an email to the Swedish clinic, requesting access to the relevant patient CT scans. After a brief check-up (patient validation, outpatient surgical facility validation, and Maltese doctor validation), the imagery technician from the Swedish clinic returns an email to the Maltese doctor with a web link to the Swedish Picture Archiving and Communication System (PACS) server, allowing access to the patient's CT scans. The Maltese doctor receives the email and, using the enclosed web link, is able to access the Swedish clinic's PACS server to view the patient's CT scans and proceed with the adequate treatment.

Aware of this process to share healthcare data across borders, a cybercriminal sends fake emails impersonating several doctors in healthcare organisations to the Swedish clinic aiming to acquire credentials to access the PACS web server data. The Swedish clinic fails to verify that the received emails are not digitally signed by a trusted healthcare organisation and does not follow the proper validation procedure, thus replying to the sender with a web link that grants access to the PACS. In addition, because the Swedish clinic does not use encrypted email (e.g., no TLS support), the cybercriminal is able to intercept emails, becoming knowledgeable of several web links to the PACS and intercepting the associated cross-border healthcare data exchanges. Once the exchanged medical data is intercepted and access to the PACS server is gained, the cybercriminal publishes online the details of the attack to harm the reputation of the healthcare organisations involved in the cross-border exchange and asks the Swedish clinic to pay for the return of the stolen medical data.

As a result of this cyberattack, and to prevent further patient data breaches, the IT Department of the Swedish clinic immediately implements the order to suspend the cross-border healthcare service. It also starts working on ways to secure the PACS server and strengthen its remote access, as well as to implement a secure cross-border healthcare data exchange service (use of digital signatures).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Impact

The use case *Intercepting Cross-border Healthcare Data Exchange* directly impacts the clinic's operations, causing a **loss of availability** of a specific healthcare service (the cross-border healthcare service) and the **violation of the confidentiality of the patients' data**. The attack's expected recovery time is estimated to be **3 working days** for reinstating the affected patients' imagery records. However, there is no estimate to re-establish the cross-border healthcare data exchange service, since the affected organisation considers it a high-risk endeavour. Moreover, there is harm to the clinic's reputation and the undermining of the patients' trust in modern online healthcare services.

SPHINX Role and Added-value Benefits

Dealing with the use case *Intercepting Cross-border Healthcare Data Exchange*, the SPHINX System is relevant in the cybersecurity certification of the PACS server and the cross-border healthcare data exchange service (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the clinic), in the identification of system vulnerabilities, namely concerning the non-secure online access to the PACS server (SPHINX vulnerability assessment and real-time cyber risk assessment tools), in the identification of the use of non-encrypted email communications (SPHINX data traffic monitoring and anomaly detection tools), in the prevention of storing non-encrypted personal data on the PACS server (SPHINX homomorphic encryption tool), in the prompt identification of unauthorised access attempts to the PACS server data (SPHINX anomaly detection tool), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tools).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Intercepting Cross-border Healthcare Data Exchange*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A Swedish clinic implements a cross-border healthcare data exchange service to deliver improved patient care. Although a validation procedure is in place, the online service is based on non-encrypted email communications and non-secure web links to access the clinic's servers.	SPHINX performs a cybersecurity verification, which includes (1) a vulnerability assessment of the IT infrastructure to identify existing vulnerabilities and (2) a risk assessment to estimate prevailing risks if non-secure protocols, such as open HTTP and plain email (without TLS), are used. SPHINX reports to the IT department the results of the verification, namely the IT ecosystem's major vulnerabilities, ensuring that the IT department is aware of them and may take adequate protection measures. SPHINX certifies the devices, components and services, including the PACS server and the cross-border healthcare data exchange service. If the devices, components and services fail the certification process and are considered non-secure, a list of their vulnerabilities is given, together with the appropriate measures to solve the identified vulnerabilities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Pre-Attack Phase	A cybercriminal becomes aware of the implemented procedure supporting the cross-border healthcare data exchange service.	The SPHINX Homomorphic Encryption tool prevents the storing of personal data on the PACS server and only allows users to search in the encrypted domain with confirmed user credentials.
Attack Phase	A cybercriminal sends fake emails impersonating several foreign doctors to the Swedish clinic aiming to acquire credentials to access the clinic's PACS web server data. The clinic does not follow the proper validation procedure and replies to the sender with web links that grant access to its PACS. In addition, the cybercriminal is able to intercept the emails requesting access to the cross-border service and intercepts the associated cross-border healthcare data exchanges. The cybercriminal publishes online these details and asks for payment to return the stolen data.	The SPHINX Homomorphic Encryption and Data Traffic Monitoring tools recognise abnormal and suspicious connections from outside the clinic to the PACS. Then, the SPHINX Decision Support System recommends the transfer of the computer providing the remote connection to a restricted network environment for further inspection. The computer is denied access to the clinic's healthcare infrastructure network services. SPHINX Data Traffic Monitoring and Data Anomaly tools detect non-encrypted email exchanges from external entities targeting specific staff and unauthorised access attempts to the PACS server data. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying potential compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The clinic's IT Department immediately suspends the cross-border healthcare service. The IT department starts working on ways to secure the PACS server and strengthen its remote access, as well as to implement a secure cross-border healthcare data exchange service (use of digital signatures).	SPHINX collects relevant attack-related data, including source and attack method, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 37: SPHINX Role and Added-value Benefits in the Use Case Intercepting Cross-border Healthcare Data Exchange

4.17 UC17: Accessing Health Data from a Fitness Tracker

Use Case 17: Accessing Health Data from a Fitness Tracker	
Scope	
Application Scenario	**Sharing and Exchange of Healthcare Information**
Attack	
Threat Type	**Malicious action – Eavesdropping**
Threat Actor(s)	**Remote attackers – Hacktivists**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**WiFi protocol;**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 17: Accessing Health Data from a Fitness Tracker	
	Non-compliance to security procedures
Critical Healthcare Assets	
Affected Asset(s)	**Mobile user devices;** **Healthcare data**
Criticality of Affected Asset(s)	**Critical**

Table 38: Key Features of the Use Case Accessing Health Data from a Fitness Tracker

Use Case Description

In order to improve the quality of diagnosis and follow-up of patients, an orthopaedic centre recommends the use of (GNSS-enabled) fitness tracker devices to monitor and store health information, including daily distance travelled, calories, hours of sleep and heart rate. The centre medical staff recommends a WiFi-enabled fitness tracker that is capable to directly connect to the centre's WiFi and communicate with the centre's server to send information.

A hacktivist who is an advocate of natural medicine and against the use of technology in medicine is aware of the growing use of fitness trackers for health purposes at the orthopaedic centre and is determined to expose the dangers of using mobile devices, by exploiting the vulnerabilities associated to wireless communications.

Aware of the orthopaedic centre network's SSID, the hacktivist creates a *replica* of the centre's WiFi by creating a WiFi access point (AP) with the same SSID as the centre's. The replicated WiFi network is configured in a way that allows all connected fitness tracker devices to also access the orthopaedic centre's *real* network (man-in-the-middle attack). Once a fitness tracker device is connected, the *replica* network captures all traffic. With a packet analyser software, the hacktivist eavesdrops the communication between the fitness tracker and the orthopaedic centre's server. Given that the device manufacturer secured communications, using an encryption mechanism based on an already known symmetric algorithm that uses plain HTTP without TLS, the hacktivist is able to access the content of the information exchange, including the patient's personal health data, such as heart rate and location. Moreover, the hacktivist is then able to access and change the patient's information sent to the orthopaedic centre's *real* network server, registering anomalous heart rate measurements, worrisome physical activity data and fake location data that raises alarm among the centre's medical staff.

Once this attack is detected by the orthopaedic centre's IT department, a statement is issued to the patients who were at the clinic on the day of the attack, recommending the return of all the fitness tracker devices that are then sent to the devices' manufacturer for the integration of adequate security measures.

Attack Impact

The use case *Accessing Health Data from a Fitness Tracker* directly impacts the orthopaedic centre's quality of service, as it implemented a programme supporting the use of fitness trackers and App for patient follow-up and caused a **violation of the confidentiality and of the integrity of the patients' data**. The integrity and credibility of the centre is also affected by having recommended a device and App that jeopardises the patients' private lives, for it as also possible for the attacker to locate and harass individual patients. Further, also the device manufacturer is deeply affected by the attack, once the information is leaked and other customers demand security assessments.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

SPHINX Role and Added-value Benefits

Dealing with the use case *Accessing Health Data from a Fitness Tracker*, the SPHINX System is relevant in the cybersecurity certification of connected devices (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the orthopaedic centre), in the identification of vulnerable protocols in critical assets (SPHINX sandbox tool), in the early detection of the attack by performing continuous monitoring of the network's activity and WiFi traffic (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Accessing Health Data from a Fitness Tracker*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	An orthopaedic centre recommends the use of fitness trackers and a tracker App to improve patient follow-up, unaware of the applicable security conditions. The centre medical staff recommends a WiFi-enabled fitness tracker that is capable to directly connect to the centre's WiFi and communicate with the centre's server.	SPHINX conducts a validation assessment of connected devices, having them deployed in the SPHINX Sandbox and running the automated cybersecurity certification module. The certification module detects and reports to the IT department the system's major vulnerabilities (use of plain HTTP connections), ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	A hacktivist acquires and sets-up the hardware and software to replicate the centre's WiFi network.	
Attack Phase	A hacktivist at the orthopaedic centre uses a WiFi AP to lure fitness tracker devices into connecting to it. The attacker eavesdrops the communication and is able to capture data from the devices, accessing its content and being able to alter the information that is then forwarded to the centre's server.	By performing continuous monitoring of the network's activity, SPHINX detects the presence of a source device (the WiFi AP connected to the centre's network) that is not registered in the assets inventory. SPHINX detects the use of plain HTTP in the exchange of data to the centre's server. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department contacts all patients with a fitness tracker who were at the orthopaedic centre on the day of the attack and warns them that their tracker may have been compromised, recommending that they return the devices. These are sent to the	SPHINX collects relevant attack-related data, including details on the suspicious device used for the attack and the compromised network devices and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
	manufacturer for adequately fixing the cybersecurity vulnerability.	

Table 39: SPHINX Role and Added-value Benefits in the Use Case Accessing Health Data from a Fitness Tracker

4.18 UC18: Transfer of Medical Devices Between Healthcare Providers

Use Case 18: Transfer of Medical Devices Between Healthcare Providers	
Scope	
Application Scenario	**mHealth services**
Attack	
Threat Type	**Malicious action – Medical device tampering**
Threat Actor(s)	**Remote attackers – Cybercriminals**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Connected devices;** **Non-secure network protocols**
Critical Healthcare Assets	
Affected Asset(s)	**Networked medical devices**
Criticality of Affected Asset(s)	**Critical**

Table 40: Key Features of the Use Case Transfer of Medical Devices Between Healthcare Providers

Use Case Description

A private sector hospital has a centralised monitoring system for all the pacemakers used by patients. The hospital has a collaboration protocol with a local Care Centre, by which they provide them monitoring equipment for their residents with pacemakers.

A cybercriminal group discovered a weakness in one of the networking protocols used by medical IoT devices (the RWHAT protocol that is used in some of the most critical systems in hospitals) to monitor a patient's condition and vitals. The weakness discovered allows medical data to be modified in real-time, providing false information to medical personnel.

Both healthcare facilities use the same networking protocols and the cybercriminals decide to take advantage of the lack of authentication of the devices connected to the network, gaining access to the monitoring devices that allowed them to mimic the vital signs of patients. After the monitoring devices are connected to the Care Centre's network, the cybercriminals have access to the whole centralised monitoring system and begin faking a massive number of cardiac arrests of patients at the same time. As a result of the attack, all medical staff is called to manage the supposed emergency.

Due to the nature of the attack, the false alarms were understood within hours, but the healthcare facilities needed to resort to offline solutions for monitoring their patients with pacemakers, while the IT departments track down the compromised devices and perform network scans for traces of malicious software that could be loaded in by the cybercriminals.

Attack Impact

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

The use case *Transfer of Medical Devices Between Healthcare Providers* directly impacts the hospital's and care centre's operations, causing a **loss of availability** of specific healthcare services (monitoring of patients with pacemakers) and the **violation of the integrity of the patients' data**, following the use of compromised devices. The attack's expected recovery time is estimated to be **3 working days**, to identify the compromised medical devices and perform network scans to detect malicious software, as well as to recover the reinstate the affected patients' records.

SPHINX Role and Added-value Benefits

Dealing with the use case *Transfer of Medical Devices Between Healthcare Providers*, the SPHINX system is relevant in the cybersecurity certification of the medical devices, equipment and the pacemakers monitoring service (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the hospital), in the identification of vulnerable critical assets (SPHINX vulnerability assessment tool), in the early detection of attacks by identifying anomalous behaviour in tampered devices (SPHINX anomaly detection tool), in the prompt alerting of relevant IT responsible as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Transfer of Medical Devices Between Healthcare Providers*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A private hospital has a centralised monitoring system for all the pacemakers used by patients. The hospital has a collaboration protocol with a local Care Centre, by which they provide them monitoring equipment for their residents with pacemakers.	SPHINX performs a thorough cybersecurity certification of the medical devices before allowing them access to the network. Only when the medical devices receive SPHINX's approval for full security compliance, are they connected into the network. SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including industry standards for newly acquired devices, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Pre-Attack Phase	The monitoring devices use the RWHAT networking protocol that presents a vulnerability, which allows the modification in real-time of the data displayed by the device.	
Attack Phase	Cybercriminals decide to take advantage of the lack of authentication of the devices connected to the network, gaining access to the monitoring devices. Once the devices are connected to the Care Centre's network, the cybercriminals have access to the whole	The SPHINX Anomaly Detection tool detects suspected and anomalous activity involving connection attempts to the centralised monitoring system. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying the originating

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
	centralised monitoring system and begin faking a massive number of cardiac arrests of patients at the same time.	and the potential destination compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The healthcare facilities resort to offline solutions for monitoring their patients with pacemakers, while the IT departments identify the compromised devices, perform network scans for traces of malicious software and recover the records of affected patients.	SPHINX collects relevant attack-related data, including compromised components (e.g., OS, files, protocols), attack patterns, IP packets and remote addresses, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 41: SPHINX Role and Added-value Benefits in the Use Case Transfer of Medical Devices Between Healthcare Providers

4.19 UC19: Illicit Rewriting of Patients' Medication

Use Case 19: Illicit Rewriting of Patients' Medication Prescription	
Scope	
Application Scenario	**eHealth Services**
Attack	
Threat Type	**Malicious action – Man-in-the-middle attack**
Threat Actor(s)	**Remote attackers – Opportunistic**
Attack Vector(s)	**Interaction with users**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 42: Key Features of the Use Case Illicit Rewriting of Patients' Medication

Use Case Description

A nursing home has a network that uses Hypertext Transport Protocol with Security (HTTPS) to ensure protected health information is not left non-secure in communications, which makes the IT workers believe in the security of the network communication channels.

An email attachment opened by a nurse installs a silent malware in the nursing home's IT network, capturing the healthcare information exchange between healthcare professionals. The hacker identifies the HTTP and HTTPS traffic and because the internal WAN certificates are not frequently changed, the hacker manages to capture one of them. And thus, the information exchange with the HTTPS channels passes through the malware before reaching the destination and the malware is capable of decrypting the exchanged information, change it, encrypt the changed information and send it to the original destination.

This malware captures the information sent from a medical doctor to a nurse, explaining the medication to be

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

given to specific patients. The malware changes the indications provided by the medical doctor and presents a new set of instructions to the nurse that follows it. The attack negatively impacts the treatment and the recovery of the patients.

The unusual patients´ recovering scenarios alert the medical team that decide to search for its causes. Rapidly, by analysing the medication information, the medical doctor identifies the mismatch in the medication administrated to the patients and the situation is corrected.

The IT department is contacted to clarify why the information on the doctor's email instructions was changed and proceeds to assess the nursing home's network and communications. The malware is identified and the IT staff proceeds with cleaning the full network.

Attack Impact

The use case *Illicit Rewriting of Patients' Medication* directly impacts the nursing home's quality of service, causing the **loss of data integrity and confidentiality** of the patient data. The attack affects the **healthcare organisation**, namely the delivery of a treatment plan with prescribed medication and causing additional treatment and longer recovery periods. In addition, this attack not only undermines the healthcare organisation's trust in its communications network but also weakens the patient's trust in the services provided by the healthcare organisation, impacting negatively the organisation's reputation. Moreover, this is an attack associated with a very long time-to-recover index, for all the changed data have to be identified.

SPHINX Role and Added-value Benefits

Dealing with the use case *Illicit Rewriting of Patients' Medication*, the SPHINX System is relevant in the identification of vulnerable critical assets (SPHINX vulnerability assessment and real-time cyber risk assessment tools), in the early detection of the attack by performing continuous monitoring of the web traffic activity (SPHINX data traffic monitoring, anomaly detection and intrusion detection tools), in the identification of the attack based on malware patterns (via the SPHINX knowledge base tool) in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Illicit Rewriting of Patients' Medication*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	The nursing home has HTTPS network communication, which makes the IT team think that the information exchanged across the network is secure.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure and monitors the use of non-encrypted communications (SPHINX maintains a database of HTTP and HTTPS internal WAN application connections and certificates, including their time validity), reporting to the IT department the system's major vulnerabilities and ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Pre-Attack Phase	A nurse opens an unsuspicious email attachment that has malware embedded.	
Attack Phase	The malware silently reads the communication and changes the content of an email providing details on how to administer medication. The changes in the prescribed medication negatively impacts the patients' recovery and health outcomes.	SPHINX continuously monitors the end-to-end communication in the network (SPHINX maintains a record of the communication protocol sequence of the application's main digital transactions) and identifies the malware that compromises communication, using the malware patterns provided by the knowledge base. SPHINX generates an alert to warn the IT department of the malware detection. SPHINX identifies the use of non-encrypted communication between systems. SPHINX generates an alert to warn the IT department of the detected vulnerability. SPHINX provides the IT department with a detailed report of the attack activity, identifying potential compromised assets and suggesting proper course of action for recovery and mitigation measures (e.g., frequent change of certificates).
Recovery Phase	The IT team confirms that the medication information was changed due to malware and starts the procedure to clean the network.	SPHINX collects relevant attack-related data, including source and attack method, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 43: SPHINX Role and Added-value Benefits in the Use Case Illicit Rewriting of Patients' Medication

4.20 UC20: Compromised Workstation Allows the Scanning of Hospital Network

Use Case 20: Compromised Workstation Allows the Scanning of Hospital Network	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Malicious action – Malware**
Threat Actor(s)	**Remote attackers – Opportunistic**
Attack Vector(s)	**Wired communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Non-observation of security rules by internal user**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 20: Compromised Workstation Allows the Scanning of Hospital Network	
Criticality of Affected Asset(s)	**Critical**

Table 44: Key Features of the Use Case Compromised Workstation Allows the Scanning of Hospital Network

Use Case Description

A hospital workstation becomes compromised as a result of an employee opening an email containing a Trojan. Planted by a Black Hat hacker, this malware provides an open backdoor through which the attacker is able to launch a network scanner. The Black Hat hacker's scanner starts collecting information about the hospital's IT assets (computers, workstations, desktops and services), enabling the building of a map of the network's connected devices, while extracting detailed information concerning operating systems, browsers and network protocols.

The Black Hat hacker's intent is to identify vulnerable IT assets that could be exploited for strengthening the attacker's presence in the hospital's network, leveraging the position towards accessing sensitive health-related information such as patient data, medical bills and credit information.

As soon as the hospital's IT department becomes aware of the reconnaissance attack, its staff proceeds to identify any compromised assets and perform a clean installation of the compromised devices, whereas new access credentials are created for all users of the compromised assets.

Attack Impact

The use case *Compromised Workstation Allows the Scanning of Hospital Network* portrays the activity of a Black Hat hacker that may impact the hospital's operations, for it allows the attacker to gather information about the vulnerabilities of the hospital's IT assets. These vulnerabilities may be exploited, delivering to the attacker deeper access to the hospital's IT systems and increasing the hacker's opportunity to undermine, from the inside, the hospital's cyber defences. In this context, the black hacker could explore simple DoS attacks or sophisticated ransomware attacks or plain sale of health data. The possibilities opened through the reconnaissance attack would likely cause the **loss of availability** of all IT-dependent healthcare services, forcing the hospital's staff to fall back to paper-based operations, or the illegal retrieval of sensitive patient data hosted by the healthcare organisation, thus leading to the breach of **the data integrity and confidentiality**. The attack's expected recovery time is estimated to be **2 working days**, for identifying and cleaning all compromised devices and for producing new access credentials to all users.

SPHINX Role and Added-value Benefits

Dealing with the use case *Compromised Workstation Allows the Scanning of Hospital Network*, the SPHINX System is relevant in the identification of vulnerable critical assets and compromised assets (SPHINX vulnerability assessment tool), in the early detection of the network scanning attack by attracting activity to concealed detection tools and performing continuous monitoring of the network's activity (SPHINX honeypot and intrusion detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

case *Compromised Workstation Allows the Scanning of Hospital Network*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A hospital's administrative unit lacks cybersecurity skills and, as a result, the adopted security policies are weak, the IT network presents multiple vulnerabilities and the hospital's staff is undertrained in cybersecurity awareness and practice.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including connected devices and software that is outdated and missing security patches, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures. SPHINX deploys a honeypot to serve as an early warning system for attacks and uses it to report the different ways the malware is trying to propagate inside the network.
Pre-Attack Phase	An hospital employee clicks on an email attachment that carries a Trojan.	
Attack Phase	The Trojan malware installs a backdoor in the workstation that the employee used to view the email's attachment. The attacker uses the backdoor to launch a reconnaissance attack towards identifying vulnerable IT assets, devices and services. The gathered intelligence is uploaded to the attacker's online server. The attacker intends to use this information for strengthening the grip on the hospital's IT assets and weaken the existing cyber protection system.	SPHINX recognises a suspicious network scan of the network's internal assets stemming from the compromised workstation (using the honeypot and intrusion detection derived dataset). SPHINX generates an alert of the suspicious activity to warn the IT department, recommending the transfer of the affected computer (i.e., the computer performing the network scan) to a restricted network environment for further inspection. The compromised computer is denied access to the hospital's resources, namely the patient data. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting the proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department identifies the compromised assets and proceeds with a clean installation of all affected assets. The IT department also issues new credentials for the users of the IT assets.	SPHINX collects relevant attack-related data, including information about the infection method, which computers were scanned, which remote IP was used and traffic data logs, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 45: SPHINX Role and Added-value Benefits in the Use Case Compromised Workstation Allows the Scanning of Hospital Network

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4.21 UC21: Identifying Common Cyber Risks across Different Healthcare Organisations

Use Case 21: Identifying Common Cyber Risks across Different Healthcare Organisations	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**System failure – Software failure**
Threat Actor(s)	**Others**
Attack Vector(s)	**Wired communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Software bug in equipment software**
Critical Healthcare Assets	
Affected Asset(s)	**Networked medical devices;** **Healthcare information systems**
Criticality of Affected Asset(s)	**Highly critical**

Table 46: Key Features of the Use Case Identifying Common Cyber Risks across Different Healthcare Organisations

Use Case Description

The National Health Ministry decided to procure 20 magnetic resonance imaging (MRI) scanners for hospitals that are part of the public national health service, based on an economic efficiency rationale. Because the procurement was successful to establish economies of scale, the same process was repeated and the same MRI scanners are now installed in all the 96 entities of the public hospitals' network.

In one of the first public hospitals to benefit from the MRI scanner, the healthcare professionals start to notice a decline in the scanner's performance. They inform the hospital's IT department that contacts the MRI scanner supplier. The supplier claims the MRI scanner is in perfect working condition, despite being a 17-year old version. Notwithstanding the supplier's assurances, the following day, the MRI scanner begins to continuously transmit MRI images in a loop, causing the overload of the PACS server in a matter of minutes. The hospital has to shut down the MRI scanner to interrupt the image transmissions, but it already lost access to the millions of CT scans, MRIs and X-rays stored in the PACS, significantly affecting the delivery of patient care.

Two days later, the hospital's IT staff manages to bring back online the PACS server, but continues to work together with the MRI scanner supplier's technicians to reconnect the MRI scanner. They learn that a bug in the original code caused a malfunction: it had set a ceiling of 50 million scans for the machine and when the equipment reached this figure, it overloaded and entered in a continuous loop transmitting MRI imaging. With the provided details, the supplier was able to develop a software patch to correct the situation. Two weeks later, when the hospital's IT staff applied the software patch, the MRI scanner became again operational.

The IT department registered the cyber incident in the hospital's blockchain-based threat registry, which shared the information with the threat registries of other healthcare organisations. The IT departments of the other public hospitals that owned the same MRI scanner became therefore aware of this risk and were able to take preventive measures (request the supplier for the software patch to solve the vulnerability) to avoid the same system failure experienced by the hospital.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Impact

The use case *Identifying Common Cyber Risks across Different Healthcare Organisations* directly impacts the hospital's care delivery, as well as the reputation of the medical equipment manufacturer whose equipment severely affects the healthcare organisation's IT infrastructure, namely the PACS server. Further, the hospital's operations are impacted, due to the **loss of availability** of the MRI scan service as well as of the access to the PACS server, as a consequence of MRI scanner system failure. The attack's expected recovery time is estimated to be **2 working days**, for placing the PACS server back online and restoring the healthcare professionals' access to millions of stored CT scans, MRIs and X-rays, and another **2 weeks**, for patching the vulnerability found in the MRI scanner and reconnecting it to the hospital's network.

SPHINX Role and Added-value Benefits

Dealing with the use case *Identifying Common Cyber Risks across Different Healthcare Organisations*, the SPHINX System is relevant in the cybersecurity certification of medical equipment (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the hospital), in the identification of system vulnerabilities, including connected medical equipment (SPHINX vulnerability assessment tools), in the early detection of the attack by identifying suspicious network activity (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tools). The SPHINX System also assists in sharing the details of the cyber incident to the other connected healthcare organisations, namely the public hospitals that also own the same MRI scanner and are therefore exposed to the same cyber risk, allowing them to take preventive measures (SPHINX blockchain-based treat registry tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Identifying Common Cyber Risks across Different Healthcare Organisations*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	The National Health Ministry decided to procure 20 MRI scanners for hospitals that are part of the public national health service, based on an economic efficiency rationale. Because the procurement was successful to establish economies of scale, the same process was repeated and the same MRI scanners are now installed in all the 96 entities of the public hospitals' network.	SPHINX performs a cybersecurity certification of the medical equipment, including the MRI scanner and the PACS servers, before being deployed in the hospital's network. If the devices, components and services in the network fail the certification process and are considered non-secure, a list of their vulnerabilities is presented, together with the appropriate measures to solve the identified vulnerabilities. SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including connected medical equipment, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
		The SPHINX Blockchain-Based Threat Registry tool provides auditable evidence of potential attacks vectors to critical assets.
Pre-Attack Phase	In one of the first public hospitals to receive the MRI scanner, healthcare professionals notice a decline in the scanner's performance and inform the hospital's IT department that contacts the MRI scanner supplier. The supplier claims the MRI scanner is in perfect working condition, despite being a 17-year old version.	
Attack Phase	The MRI scanner begins to continuously transmit MRI images in a loop, causing the overload of the PACS server in a matter of minutes. The hospital has to shut down the MRI scanner to interrupt the image transmissions, but it already lost access to the millions of CT scans, MRIs and X-rays stored in the PACS, significantly affecting the delivery of patient care.	SPHINX recognises the abnormal network activity and identifies the MRI equipment responsible for the PACS server overload. SPHINX generates an alert of the suspicious activity to warn the IT department of the identity of the affected equipment. The IT staff transfers the compromised MRI scanner to an isolated network environment (SPHINX Sandbox) for further inspection. The MRI scanner no longer accesses the hospital's network. The incident is recorded in the SPHINX Blockchain-Based Threat Registry, becoming an information accessible across all entities with access to the SPHINX blockchain-based tool. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT staff manages to bring back online the PACS server and continues to work together with the MRI scanner supplier to reconnect the MRI scanner. They learn that a bug in the original code caused the malfunction. The supplier develops a software patch to correct the situation. Two weeks later, the MRI scanner is operational again. The IT department registers the cyber incident in the hospital's blockchain-based threat registry, sharing the information with the threat registries of other healthcare organisations. Those owning the same MRI scanner became aware of the risk and take preventive measures (request the supplier for the software patch to solve the vulnerability) that avoid system failure.	SPHINX collects relevant attack-related data in the SIEM and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and the obligation to report data breaches to the authorities, while providing lessons learned to improve cybersecurity, training activities and prevent future attack occurrences. SPHINX shares details of the cyber incident with other healthcare organisations through the Blockchain-based Threat Registry tool, allowing them to take preventive measures to avoid the system failure.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table 47: SPHINX Role and Added-value Benefits in the Use Case Identifying Common Cyber Risks across Different Healthcare Organisations

4.22 UC22: Digital Identity Theft of a Medical Doctor

Use Case 22: Digital Identity Theft of a Medical Doctor	
Scope	
Application Scenario	**eHealth Services**
Attack	
Threat Type	**Malicious action – Social engineering**
Threat Actor(s)	**Malicious external users**
Attack Vector(s)	**Interaction with users (social engineering)**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**User with privileged access**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare information systems**
Criticality of Affected Asset(s)	**Critical**

Table 48: Key Features of the Use Case Digital Identity Theft of a Medical Doctor

Use Case Description

A medical doctor lost the professional identity card that, combined with a username and password, gives full access to the hospital's network. The medical doctor did not report the theft to the hospital's IT service but shared this information with a few of the patients. The following day, the medical doctor received a trustworthy phone call from one of the patients pretending to be the director of the hospital's IT service. The fake hospital IT director (the patient) asked whether the medical doctor had lost the professional identity card, since an attempt to use it and enter into the hospital network had been identified. As the medical doctor confirmed it, the fake hospital IT director (the patient) asked for the login and password in order to cancel the card and make a new one. The medical doctor provided the user name and password to the fake hospital director (the patient) to quickly solve the case.

With the medical doctor professional identity card, user name and password, the patient gains access to the hospital's network and installs a malware that rapidly shuts-down the entire hospital services. As the attack spread, the hospital's medical, nursing and accounting staff are ordered to stop using the digitalised systems and the IT infrastructure and switch to paper-based operations.

Responding to the attack, the hospital's IT service shut down the whole IT infrastructure and proceed with a clean installation of computers, resorting to backup systems to partially recover hospital services and records.

Attack Impact

The use case *Digital Identity Theft of a Medical Doctor* directly impacts the hospital's quality of service, causing the **loss of availability** of all healthcare services that are IT-dependent and forcing the clinic's staff to revert to paper-based operations, where possible. The attack affects the **healthcare organisation**, namely the delivery of medical care services, and determines the activation of costly alternative healthcare services (transfer patients to another hospital to perform necessary treatments) to handle adequate healthcare delivery. In

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

addition, this attack not only undermines the healthcare organisation's trust in the hospital network but also weakens the patient's trust in the services provided by the healthcare organisation, possibly impacting negatively on the patient's recovery and health outcomes.

SPHINX Role and Added-value Benefits

Dealing with the use case *Digital Identity Theft of a Medical Doctor*, the SPHINX System is relevant in the presentation of best cybersecurity practices, including password protection and reporting stolen identity cards (SPHINX knowledge base), in the early detection of the attack by performing continuous monitoring of the network traffic activity and detecting a suspicious access (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX real-time cyber risk assessment and interactive dashboard tools), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Digital Identity Theft of a Medical Doctor*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	Medical doctors have a professional identity card that, combined with the user name and password, provide full access to the hospital's IT network.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including access policies, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures in emergency situations.
Pre-Attack Phase	The medical doctor lost the professional identity card and failed to report it to the hospital's IT service.	The SPHINX Knowledge Base contains attack patterns and associated mitigation actions. Using this data, SPHINX components generate best practices that can be used as a base for periodic instruction sessions with hospital employees. Hospital employees are made aware that passwords are not to be shared and that, in this specific situation, they should communicate to the IT department as soon as possible that there is a lost identity card so it can be cancelled.
Attack Phase	A patient impersonates the hospital's IT director to retrieve the medical doctor's user name and password. With these assets, the patient/attacker installs a malware that shuts down the entire hospital services and leaving the hospital's staff to perform paper-based operations.	SPHINX data traffic monitoring tool raises an alert when it detects a suspicious connection to a server (an access using a ID card reported stolen), in order to warn the IT department. SPHINX decision support system analyses the alert and generates a list of possible courses of action, including isolating the computer from the network. Both the alert and the suggested actions are presented via the SPHINX Interactive Dashboard. SPHINX provides the IT department with a detailed report of the attack activity, identifying potential compromised assets and suggesting proper course of action for recovery and mitigation measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Recovery Phase	Responding to the attack, the hospital's IT service shuts down the whole IT infrastructure and proceeds with a clean installation of computers, resorting to backup systems to partially recover hospital services and records.	SPHINX collects relevant attack-related data, including source and attack method and the network traffic data from a relevant interval prior to the alert, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 49: SPHINX Role and Added-value Benefits in the Use Case Digital Identity Theft of a Medical Doctor

4.23 UC23: Attack to Public Healthcare Data Repositories

Use Case 23: Attack to Public Healthcare Data Repositories	
Scope	
Application Scenario	**Sharing and Exchange of Healthcare Information**
Attack	
Threat Type	**Malicious action – Hijacking**
Threat Actor(s)	**Insider threat**
Attack Vector(s)	**Physical interaction with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability	**Public healthcare data repositories**
Critical Healthcare Assets	
Affected Asset(s)	**Healthcare data repositories** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 50: Key Features of the Use Case Attack to Public Healthcare Data Repositories

Use Case Description

Hospitals use remote healthcare data repositories hosted by the regional healthcare authority to ensure access to secure regional records of patient information. Hospital staff accesses these regional databases to retrieve medical records that are needed. The databases are monitored and controlled by database managers who ensure that no unauthorised activity can take place. They oversee incoming data types to block viruses that can be passed without the knowledge of a system user and they audit requests made on a database to ensure compliance with prevailing policies and rights.

The database manager is curious about a friend's health. After contacting the hospital and not receiving a positive response due to doctor-client non-disclosure information agreement, the database manager decides to take advantage of the managerial position and uses the privileges to access the regional database. The database manager opens the database and realises that it does not contain any names and all information is placed against medical record numbers, with most of the personal credentials anonymised. The database manager, in need of more time and privacy, decides to stop and continue after working hours. When the work is resumed, the database manager quickly refines the search with a specific age group, thus reducing the overall

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

search space. After, the database manager runs a secondary search on this reduced search space and looks for a particular location approximation. This search narrows down the search space to three individuals with 2 women and 1 man as the final outcome. The database manager looks into the medical record of the single man and knows that it is the friend's records. The database manager clears the audit trail and now owns the healthcare record without requesting anyone for it. The database manager uses the privileged credentials to offer a service to individuals who want such information for a particular price set.

Throughout this process, the hospital remains unaware that the security of the regional healthcare data repositories has been breached and they maintain the use of the service until someone reports it. Once the hospital knows about the compromised access to the regional healthcare databases, the database manager is fired, the data breach is communicated to the regional healthcare authority and the hospital's accesses to the regional healthcare data repositories are changed.

Attack Impact

The use case *Attack to Public Healthcare Data Repositories* exploits the remote access to regional healthcare data repositories by insiders for personal (financial) gain. This attack directly impacts the hospital's care services, resulting in the **loss of data confidentiality** and a violation of the hospital's privacy compliance policy, posing hefty fines to the hospital under the EU General Data Protection Regulation. At the same time, the attacker may use the access to sensitive data to exploit vulnerabilities of the patients in the dataset for personal gain and/or sell the information to interested parties.

SPHINX Role and Added-value Benefits

Dealing with the use case *Attack to Public Healthcare Data Repositories*, the SPHINX System is relevant in the assurance that the sensitive patient data is securely encrypted (SPHINX anonymisation and privacy and homomorphic encryption tools), in the early detection of attacks by identifying the suspicious user behaviour (SPHINX anomaly detection tool), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures, including blocking the attack (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Attack to Public Healthcare Data Repositories*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	The hospital uses remote regional healthcare databases to store relevant patient information.	
Pre-Attack Phase	The database manager is curious about a friend's health condition.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Attack Phase	The database manager uses privileged credentials to exploit the regional healthcare repositories and access the friend's records. The data manager continues to use the privileged access to offer a service to individuals who want patient information for a particular price set.	SPHINX encrypts all data stored onto the healthcare data repositories thus mitigating the chances of an attacker reading into the stored dataset. It also provides a way of performing encrypted searches, thus mitigating the possibility of someone being able to identify what is being searched in the encrypted dataset. SPHINX detects suspicious user behaviour, caused by suspicious access to sensitive data after normal working hours. SPHINX generates an alert of the suspicious activity to warn the IT department and identifies the originating and destination computers. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	Once the hospital knows about the compromised access to the regional healthcare databases, the database manager is fired, the data breach is communicated to the regional healthcare authority and the hospital accesses are changed.	SPHINX collects relevant attack-related data, including the compromised hospital accesses to regional healthcare databases, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences

Table 51: SPHINX Role and Added-value Benefits in the Use Case Attack to Public Healthcare Data Repositories

4.24 UC24: Theft of Patient Data using the Telemedicine System

Use Case 24: Theft of Patient Data using the Telemedicine System	
Scope	
Application Scenario	**mHealth Services**
Attack	
Threat Type	**Malicious action – Man-in-the-middle attack**
Threat Actor(s)	**Remote attackers – Opportunistic**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Web Real-Time Communication**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment;** **Healthcare information systems;** **Healthcare data repositories;** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 52: Key Features of the Use Case Theft of Patient Data using the Telemedicine System

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case Description

Knowing that telemedicine contributes to universal healthcare coverage by promoting access to quality and cost-effective health services in any location, a regional hospital in a rural area has made available to its patients a telemedicine service, in order to support isolated populations, including geriatric and mobility impaired individuals, to make remote consultations and to contact specialists who are only available in other hospitals. The hospital's Telemedicine System uses Web Real-Time Communication (WebRTC) and Datagram Transport Layer Security (DTLS) to generate keys for the Secure Real-Time Transport Protocol (SRTP) media session. Both Web and application accesses are protected by verified email and password.

An elderly patient, who suffers from high blood pressure and whose medication has recently been changed, has a telemedicine video call scheduled with the family physician, to see how the adaptation to the new medication is unfolding. On the day of the appointment, the doctor enters the hospital's system, which is connected to the Internet via a Virtual Private Network (VPN), and is notified of the telemedicine appointment. The doctor checks the patient's Electronic Medical Record (EMR). After taking the new medication each morning, the patient opens the web browser and logs into the scheduled telemedicine video call with the hospital's doctor. The video call consult starts.

Earlier in the day, an attacker joined the hospital's network and found that the hospital's VPN is leaking the customer's IP address via a WebRTC bug. Having found an active media session, the attacker launches a man-in-the-middle (MitM) attack, compromising the signalling server. So, instead of the signalling server only connecting the doctor to the patient, the patient and the doctor are also connected to the attacker without noticing it. When the patient called the doctor, establishing a WebRTC Peer Connection, the attacker received a Session Description Protocol (SDP) offer and created a new Peer Connection to the doctor, sending to the doctor a SDP offer. As a result, there are two Peer Connections instead of one, and both terminate on a MitM JavaScript application. The attacker accesses not only the audio and image of the video call but also the patient's EMR data, compromising the EMR integrity. Then, the attacker introduces a crypto-ransomware into the hospital's network, threatening to destroy the patient data.

The hospital's IT department has to shut down the network, disconnect all computers and proceed with their reinstallation. In the meantime, the hospital activates the contingency plan to obtain the EMRs in paper format.

Attack Impact

The use case *Theft of Patient Data using the Telemedicine System* impacts the healthcare service provider's operations, causing a **loss of availability** of healthcare databases, patient data and of healthcare services, namely those requiring IT-based systems, including the telemedicine system. The attack directly impacts the hospital's quality of service, causing a **violation of the confidentiality of the patients' data.** The attack affects the **healthcare organisation** and its **patients**, as they no longer are able to receive specific healthcare services. The attack's expected recovery time is estimated to be **1 or 2 months**, depending on the extent of the infection and on the time spent to reinstall the backup files to reset the encrypted data. Because the attack compromised the C-I-A (confidentiality, integrity and availability) of electronic medical records, patients are wary of using the hospital's healthcare services again.

SPHINX Role and Added-value Benefits

Dealing with the use case *Theft of Patient Data using the Telemedicine System*, the SPHINX System is relevant in the cybersecurity certification of the medical devices, equipment and the telemedicine service, identifying the compliance with cybersecurity standards (SPHINX sandbox tool) before being deployed in operational

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

environments (i.e., the hospital), in the identification of vulnerable critical assets (SPHINX vulnerability assessment tool), in the detection of suspicious network activity (SPHINX anomaly detection tool) and in the early detection of attacks by identifying the compromised computers (SPHINX honeypot and intrusion detection tools). The SPHINX System also assists in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tools).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Theft of Patient Data using the Telemedicine System*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A hospital implements a WebRTC Telemedicine service, allowing doctors to perform remote consultations with patients from isolated locations.	SPHINX Vulnerability Assessment as a Service tool periodically conducts a vulnerability assessment of the full IT infrastructure, including the VPN and file exchange protocols, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures. SPHINX also checks if the telemedicine video call server ensures secure connection via SSL/TLS encryption protocols and multi-layer security with AES 256 end-to-end encryption. The SPHINX Security Information and Event Management regularly monitors the entire hospital network and verifies whether the telemedicine software complies with applicable certification standards.
Pre-Attack Phase	An attacker plans a large-scale ransomware attack targeting hospital data, exploiting a vulnerability in the telemedicine system.	
Attack Phase	The attacker intercepts a telemedicine consultation between a doctor and a patient, by launching a MitM attack that compromises the signalling server. As a result, two Peer Connections are established, both terminated on a MitM JavaScript application. The attacker accesses the audio and image of the video call. Having control of communications, the attacker introduces a crypto-ransomware into the hospital's network. Once activated, the ransomware propagates through the computer network of the hospital.	By performing continuous monitoring of the network's activity, SPHINX detects suspicious accesses and generates an alert to warn the IT department. The SPHINX Anomaly Detection and Security Information and Events Management tools detect unauthorised network scan activities, identifying the source machine, as well as the suspicious network activity caused by the cryptoworm propagation, identifying the source devices. The SPHINX Security Information and Events Management also identifies the presence and category of the cryptoworm (via ClamAV interface). The SPHINX alert identifies the affected computers, allowing the IT staff to transfer them to an isolated network environment for further inspection. The SPHINX Analytical Engine raises the user's awareness to the attack based on the visualisations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
		(e.g., bar, pie charts) brought forth by the ID. SPHINX generates an alert of the suspicious activity to warn the IT department. The SPHINX Security Information and Events Management provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures. The SPHINX Decision Support System provides a set of actions to remove the malware from each affected asset and bring the system back to normal operational level. It also provides the correlation of the system's vulnerabilities with the attack specifics and suggests how to eliminate them.
Recovery Phase	The IT department shuts down the network, disconnects all computers and proceeds with their reinstallation. The hospital activates the contingency plan to obtain patients' EMRs in the paper format.	The SPHINX Forensic Data Collection Engine collects relevant attack-related data, including details on the computer used for the attack, the compromised network devices and the used remote IP address, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 53: SPHINX Role and Added-value Benefits in the Use Case Theft of Patient Data using the Telemedicine System

4.25 UC25: Transfer of Patients Between Healthcare Organisations

Use Case 25: Transfer of Patients Between Healthcare Organisations	
Scope	
Application Scenario	**Sharing and Exchange of Healthcare Information**
Attack	
Threat Type	**Malicious actions – Hijacking**
Threat Actor(s)	**Insider threat**
Attack Vector(s)	**Wired communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Lack of security controls within the network;** **RDS vulnerability**
Critical Healthcare Assets	
Affected Asset(s)	**IT and networking equipment;** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 54: Key Features of the Use Case Transfer of Patients Between Healthcare Organisations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case Description

A patient hospitalised in a Cardiology clinic has to be transferred to the region's hospital in order to undergo a coronary angiography examination. Once the patient arrives at the hospital, the attending cardiologist requests the patient's health data (medical records) from the clinic. The hospital's cardiologist sends an email to the clinic requesting access to MRI and CT exams (DICOM data), diagnosis reports (ICD-10 data), medication received and blood and microbiological lab test results.

The Cardiology clinic receives the email, confirms its authenticity and issues temporary credentials (user name and password) to the hospital's cardiologist that allows him read-only access to the clinic's information system. A web link within the SYZEFXIS secure network (a network linking the regional healthcare organisations) is sent via email to the hospital's cardiologist, followed by a separate email with user credentials (user name and password). Because the blood tests and DICOM data are not yet available in the clinic's database, the clinic's IT staff sets up access via a Remote Desktop Software (RDS) to a virtual machine with a LIS and PACS clients installed to enable the viewing of the requested data.

A dissatisfied administrative employee at the clinic decides to use IT skills to augment personal revenues by selling patient data in the dark web. With access to the clinic's network, the dissatisfied employee runs a software that captures network packets and, due to the use of non-secure (non-encrypted) communications, is able to retrieve the web link and user credentials issued by the clinic to the region's hospital. Moreover, the dissatisfied employee uses a network scanner that discovers the machines accessible via RDS, which has known vulnerabilities that the employee decides to exploit to achieve remote code execution. The dissatisfied employee therefore accesses the clinic's patient data and steals it, advertising its sale in the dark web.

The clinic's IT department is alerted to the network scanning activities and the suspicious user behaviour and identify the machine and the user responsible for the data breach. The IT department blocks the machine's network connectivity and the dissatisfied employee is fired. New security policies and measures are implemented by the clinic, including the updating of patches of the operating system, the halt of RDS access to the IT ecosystem, the sending of user credentials in separate communications and through different communication channels (SMS, email, telephone) and the use of secure encrypted protocols (end-to-end encryption with TLS) in emails.

Attack Impact

The use case *Transfer of Patients Between Healthcare Organisations* directly impacts the clinic's operations by revealing a major patient data breach and the **violation of the confidentiality of patients' data**. Also, there is a **loss of availability** of the sharing and exchange of healthcare data service, endangering the continuity of treatment and optimal patient care in the region. The attack affects the **healthcare organisation** and its **patients**, as they learn that their personal medical information has been stolen and is being sold in the dark web. The attack's expected recovery time is estimated to be **1 or 2 months**, depending on the number of patients affected by the data breach and on the time spent to reinstall the backup files. The reputation of the clinic is profoundly affected, which reflects forward to the secure network connecting the regional healthcare organisations, putting into question the security of sharing and exchanging healthcare information between healthcare organisations.

SPHINX Role and Added-value Benefits

Dealing with the use case *Transfer of Patients Between Healthcare Organisations*, the SPHINX System is relevant in the cybersecurity certification of the healthcare data sharing and exchange service (SPHINX sandbox tool)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

before being deployed in operational environments (i.e., the clinic), in the identification of system vulnerabilities, namely concerning the non-secure online access to the database and the LIS and PACS servers (SPHINX vulnerability assessment and real-time cyber risk assessment tools), in the early detection of the attack by identifying suspicious network and user behaviour and performing analyses of digitally non-signed emails (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tool).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Transfer of Patients Between Healthcare Organisations*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A clinic implements a healthcare data sharing and exchange service to deliver improved patient care. Weak security procedures are in place, including the use of non-encrypted email communications and RDS access.	SPHINX certifies the ecosystem's devices, components and services, including the RDP access to the LIS and PACS servers and the healthcare data sharing and exchange service. If the devices, components and services in the network fail the certification process and are considered non-secure, a list of their vulnerabilities is presented, together with the appropriate measures to solve the identified vulnerabilities. SPHINX performs a cyber security verification, which includes (1) a vulnerability assessment of the IT infrastructure and (2) a dedicated real-time cyber risk assessment analysis. SPHINX reports to the IT department the results of the verification, namely the IT ecosystem's major vulnerabilities, ensuring that the IT department is aware of them and may take adequate protection measures.
Pre-Attack Phase	A clinic's dissatisfied administrative employee decides to use IT skills to steal patient data.	
Attack Phase	The dissatisfied employee runs a software that captures network packets and retrieves the web link and user credentials giving access to the clinic's information systems. Moreover, the dissatisfied employee uses a network scanner to discover virtual machines connecting to the clinic's servers that are accessible via RDS. The dissatisfied employee exploits the RDS known vulnerabilities to achieve remote code execution. The dissatisfied employee therefore accesses the clinic's patient data and steals it, advertising its sale in the dark web.	SPHINX identifies the use of non-encrypted communications between systems and the connection to the RDP, recognises the network scanning activities and the suspicious user behaviour and identifies the source machine. Since the user is logged when performing these actions, SPHINX also identifies the user perpetrating these activities. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying potential compromised assets and suggesting proper course of action for recovery and mitigation measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Recovery Phase	The clinic's IT department is alerted to the network scanning activities and the suspicious user behaviour and identify the machine and the user responsible for the data breach. The IT department blocks the machine's network connectivity and the dissatisfied employee is fired. New security policies and measures are implemented by the clinic, including the updating of patches of the operating system, the halt of RDS access to the IT ecosystem, the sending of user credentials in separate communications and through different communication channels (SMS, email, telephone) and the use of secure encrypted protocols (end-to-end encryption with TLS) in emails.	SPHINX collects relevant attack-related data (extensive list of log files originating from the devices hosting the data - web application linked via e-mail- and the compromised services - RDS server -, the vulnerability assessment results and the captured pcap files of network traffic) and delivers to the IT department a detailed report of the attack activity. End-users are able to investigate in depth the interaction of the non-desired IP address in the services along with the vulnerabilities that allowed to exploit the RDS service and examine traffic details relevant to eavesdropped connections, using pcap files, to realise the absence of encryption in the communication amongst the two institutes and also locate the specific eavesdropped connections. The report assists cyber forensic purposes and the obligation to report data breaches to the authorities, while providing lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 55: SPHINX Role and Added-value Benefits in the Use Case Transfer of Patients Between Healthcare Organisations

4.26 UC26: Exploiting Medical Equipment to Steal Exams Results

Use Case 26: Exploiting Medical Equipment to Steal Exams Results	
Scope	
Application Scenario	**Digital Transformation in Healthcare**
Attack	
Threat Type	**Malicious action – Medical device tampering**
Threat Actor(s)	**Malicious external users**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Connected medical equipment**
Critical Healthcare Assets	
Affected Asset(s)	**Networked medical devices;** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 56: Key Features of the Use Case Exploiting Medical Equipment to Steal Exams Results

Use Case Description

Benefitting from the digitisation effort in the health sector, a clinic made a large investment in certified medical equipment with secure networked capabilities, namely using secure TLS/SSL connections to exchange data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Posing as a visitor to a patient admitted to the clinic, a cybercriminal connects to the clinic's WiFi network and performs a thorough screening of connected equipment and rapidly identifies medical equipment using the openSSL version 1.0.1. The cyber-criminal is aware that this specific version of openSSL presents a serious known vulnerability and that many medical device manufacturers did not fix it with a security patch. Therefore, the attacker exploits what is known as the Heartbleed bug to obtain secret keys used in the X.509 certificates, usernames and passwords and exam result documents (i.e., sensitive data collected by the device). As a consequence, the cyber-criminal is able to access the clinic's sensitive information and steals patient data, namely the results of exams having been performed using the now compromised medical devices.

The clinic is only aware of this cyberattack when the cyber-criminal contacts the clinic administration to demand the payment of a ransom in bitcoin to return the stolen exams results. Upon this contact, the clinic's IT department identifies the compromised medical devices and disconnects them. Then, they contact the device manufacturer requesting the upgrade to be applied to the openSSL library. The affected patients are required to return to the clinic and repeat the exams.

Attack Impact

The use case *Exploiting Medical Equipment to Steal Exams Results* directly impacts the reputation and business prospects of the medical device manufacturer, who becomes rapidly associated with bad cybersecurity practices that cause its customers' networks to become vulnerable to attackers and at risk of compromising their patients' confidential data. Further, the clinic's operations are impacted, due to the **loss of the confidentiality of the patients' data**, as a consequence of the theft of the exams results. The attack's expected recovery time is estimated to be **3 working days**, depending on the time spent to identify the compromised medical equipment, install the security patch and reconnect the medical equipment to the clinic's network.

SPHINX Role and Added-value Benefits

Dealing with the use case *Exploiting Medical Equipment to Steal Exams Results*, the SPHINX System is relevant in the cybersecurity certification of medical equipment (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the clinic), in the identification of system vulnerabilities, including connected medical devices using the open SSL version 1.0.1 (SPHINX vulnerability assessment tools), in the early detection of the attack by identifying suspicious network activity, such as network scanning and high data traffic (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tools).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Exploiting Medical Equipment to Steal Exams Results*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	A medical equipment manufacturer made a large investment in introducing connectivity to its new device's portfolio. The manufacturer used the openSSL (version 1.0.1) to implement	SPHINX performs a cybersecurity certification of the medical equipment before being deployed in customer premises. The manufacturer receives a report identifying the measures to be taken to remove the cyber vulnerabilities detected and present a secure

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
	secure TLS/SSL connections, unaware of the Heartbleed bug. The manufacturer is selling its equipment to customers.	device. Only when the medical equipment receives the SPHINX approval of full security compliance, may the manufacturer sell a secure equipment (the equipment will not expose its customers to cyber vulnerabilities).
Pre-Attack Phase	Posing as a visitor to a patient admitted to the clinic, a cyber-criminal connects to the clinic's WiFi network and after screening the connected equipment, rapidly identifies the medical equipment using the openSSL version 1.0.1.	SPHINX periodically conducts a vulnerability assessment of the full IT infrastructure, including connected medical devices, and reports to the IT department the system's major vulnerabilities, ensuring that the IT department is aware of existing vulnerabilities and may take adequate protection measures.
Attack Phase	The attacker uses a Heartbleed exploit to retrieve secret keys used for the X.509 certificates, user names and passwords and exam result documents (i.e., sensitive data collected by the device like the patients' exams results). The attacker contacts the clinic to demand a ransom in bitcoin to return the stolen patient data.	SPHINX detects the vulnerability in the compromised equipment, delivers an alert and suggests their transference to an isolated network environment for further inspection. SPHINX generates an alert of the suspicious activity (network scanning, remote access to device data from an unknown computer, high data traffic from an unknown computer) to warn the IT department and provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department identifies the compromised medical equipment, disconnects them from the network and requests the manufacturer to fix the vulnerability. Once fixed by the manufacturer, the IT department reconnects the device to the network.	SPHINX collects relevant attack-related data, including the compromised network components (e.g., medical equipment and patient records) and delivers to the IT department a detailed report of the attack activity. The IT department is able to investigate in depth the vulnerabilities that caused the attack (OpenSSL v 1.0.1), the devices that exhibit similar vulnerabilities (devices provided from a particular vendor and others), and candidate eavesdropped connections (as present in the captured pcap file and indicated by anomaly detection logs) which are indicative of the stolen data. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences.

Table 57: SPHINX Role and Added-value Benefits in the Use Case Exploiting Medical Equipment to Steal Exams Results

4.27 UC27: Accessing Non-Protected Medical Data

Use Case 27: Accessing Non-Protected Medical Data	
Scope	
Application Scenario	**mHealth and Remote Patient Monitoring**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Use Case 27: Accessing Non-Protected Medical Data	
Attack	
Threat Type	**Malicious action – Man-in-the-middle attack**
Threat Actor(s)	**Remote attackers – Cybercriminals**
Attack Vector(s)	**Wireless communication with IT assets**
Vulnerability and Exploitation	
Exploited Vulnerability(ies)	**Connected medical equipment**
Critical Healthcare Assets	
Affected Asset(s)	**Networked medical devices;** **Healthcare data**
Criticality of Affected Asset(s)	**Highly critical**

Table 58: Key Features of the Use Case Accessing Non-Protected Medical Data

Use Case Description

A maternity recently bought a set of medical devices that can be connected to the maternity's IT infrastructure, using a wireless network. Using these devices, the patients' health parameters may then be visualised through the devices' monitors in the patients' room, as well as in the central control at the nurses' station. As these devices are setup in the maternity's IT ecosystem, the security of the data exchanged is dependent on the security level of the transmission channel (the devices). In addition, these devices allow the additional installation of sensors from different vendors. However, the devices provide sensing data in non-encrypted manner.

In the maternity's waiting room, a hacker exploits a vulnerability in a router and gains access to the local network. The hacker deploys a packet sniffer and is able to retrieve non-encrypted data produced by the medical devices, thus gaining access to patients' sensitive medical data. Afterwards, the hacker decides to tamper with the messages and modifies the medical data being sent. The medical staff is misinformed of the patients' condition and subsequent treatments are not appropriate, risking worsening the patients' wellbeing. Only after a few days, the medical staff identifies that the data reported by the medical devices is inadequate. As a result, the medical devices are returned to the manufacturer and subjected to thorough technical review process in order to identify the source of errors and security vulnerabilities.
As a result of the attack, the manufacturer decides to integrate a component that adds a secure-trusted element into the device, taking advantage of ARM Trustzone secure capabilities[5] before transmitting data. For the manufacturer, the only architectural change is to handle this element as a new communication system, keeping the existing device unaltered.

Attack Impact

The use case *Accessing Non-Protected Medical Data* directly impacts the healthcare organisation, for the attack targets the patients' information transmitted across the maternity's network, causing the **violation of the data confidentiality and integrity** and compromising specific health monitoring services and subsequent treatments. The attack's expected recovery time is estimated to be **2 to 4 working days**, depending on the time spent to identify the compromised medical equipment, proceed with its reinstallation and reconnect the medical equipment to the maternity's network. The medical equipment technical review is estimated to be 4 to 6 weeks and the modular security patch (i.e., the new secure-trusted element) is estimated to take up to 2 days.

[5] Trustzone is a feature of ARM-V8 architecture for chips.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

SPHINX Role and Added-value Benefits

Dealing with the use case *Accessing Non-Protected Medical Data*, the SPHINX System is relevant in the cybersecurity certification of medical equipment (SPHINX 3rd party APIs and sandbox tools) before being deployed in operational environments (i.e., the maternity), in the early detection of the attack by identifying suspicious network activity associated with accessing the router and medical devices (SPHINX data traffic monitoring and anomaly detection tools), in the prompt alerting of relevant IT staff as soon as the attack is detected (via the SPHINX interactive dashboard tool), in the presentation of a detailed report on the cyberattack (SPHINX security information and event management, forensic analysis and analytical engine tools) and in the delivery of decision support instructions to the IT department staff on how to proceed to trigger and implement the adequate recovery and mitigation procedures (SPHINX decision support tools). The device manufacturer also receives the list of cybersecurity vulnerabilities of the device and may immediately proceed with implementing relevant mitigation actions (i.e., integrating a new secure-trusted element into the device).

The table below summarises the role played by the SPHINX system to counter the attack depicted in the use case *Accessing Non-Protected Medical Data*.

Attack Phases	Cybersecurity Attack	SPHINX Role and Added-value Benefits
Initial Conditions	An existing medical device provides data in a non-protected manner, trusting on network credentials to transmit data.	SPHINX performs a cybersecurity certification of the medical devices before being deployed in customer premises. The manufacturer receives a report with a list of their vulnerabilities and identifying the measures to be taken to remove them, thus securing the device.
Pre-Attack Phase	The attacker accesses the network exploring a known vulnerability in the router.	SPHINX identifies the use of non-encrypted communications between systems, which could expose sensitive and personal data.
Attack Phase	The attacker collects the data being sent in real-time by the medical devices. The attacker intercedes the data and modifies it, compromising the medical assistance being provided to patients. The IT department is alerted by the nursing staff that the data displayed in the medical devices' monitors is faulty.	SPHINX detects the presence of non-encrypted communications between systems, the connection to the router administration panel and the attempts of the new unauthorised device to enter the network. SPHINX generates an alert of the suspicious activity to warn the IT department. SPHINX provides the IT department with a detailed report of the attack activity, identifying compromised assets and suggesting proper course of action for recovery and mitigation measures.
Recovery Phase	The IT department identifies and disconnects the compromised medical devices. A new installation is sought before the devices are re-connected to the network.	SPHINX collects relevant attack-related data, including source and attack method, and delivers to the IT department a detailed report of the attack activity. The report assists cyber forensic purposes and provides lessons learned to improve cybersecurity, training activities and prevent future attack occurrences. The manufacturer receives the list of cybersecurity vulnerabilities and proceeds with implementing the mitigation actions, thus securing the device. The device passes the SPHINX certification process.

Table 59: SPHINX Role and Added-value Benefits in the Use Case Accessing Non-Protected Medical Data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4.28 SPHINX Use Cases Overview

The following image provides a traceability matrix that clearly associates the different SPHINX use cases with the application scenarios identified for SPHINX, considering the framework of critical assets, threat taxonomy and actors, attack vectors and impact that has guided the discussions among SPHINX partners in Task 2.4 - *Reference Scenarios, Pilot Operations and KPIs*. The traceability matrix is used to ensure completeness, highlighting that all application scenarios are covered by at least one SPHINX use case.

Use Cases	UC01	UC02	UC03	UC04	UC05	UC06	UC07	UC08	UC09	UC10	UC11	UC12	UC13	UC14	UC15	UC16	UC17	UC18	UC19	UC20	UC21	UC22	UC23	UC24	UC25	UC26	UC27
Application Scenarios																											
Digital Transformation in Healthcare	•		•			•		•				•			•					•	•					•	
eHealth Services				•							•			•					•			•					
mHealth and Remote Patient Monitoring Platforms					•		•		•	•			•					•						•			•
Sharing and Exchange of Healthcare Information		•															•						•		•		
Cross-border Healthcare Service Delivery																•											
Attack Type																											
Malicious actions - Malware	•		•	•				•	•				•	•						•							
Malicious actions - Hijacking		•									•												•		•		
Malicious actions - Eavesdropping																	•										
Malicious actions - Man-in-the-middle																•			•					•			•
Malicious actions - Medical device tampering					•					•								•								•	
Malicious actions - Device and Data Theft															•												
Malicious actions - Ransomware						•																					
Malicious actions - Distributed Denial of Service							•																				
Malicious actions - Social Engineering					•					•		•			•							•					
Human error												•					•										
System failure																					•						
Attack Vectors																											
Physical interaction with IT assets								•							•								•				
Wired communication with IT assets					•															•	•				•		
Wireless communication with IT assets	•	•					•		•		•		•	•		•	•	•						•		•	•
Interaction with users			•	•		•				•		•							•			•					
Attack Actors																											
Remote Attackers - Government Sponsored									•																		
Remote Attackers - Cyber Criminals						•			•					•				•									•
Remote Attackers - Cyber Terrorists			•																								
Remote Attackers - Hacktivists		•															•										
Remote Attackers - Opportunistic	•			•			•						•			•			•	•				•			
Insider threats					•			•															•		•		
Malicious external users											•	•			•							•				•	
Affected Assets																											
Healthcare information systems	•			•		•	•					•		•	•						•	•		•			
Healthcare data repositories			•			•																	•	•			
Identification system			•						•																		
Networked medical devices					•					•								•			•					•	•
Mobile user devices									•						•		•										
IT and networking equipment	•	•	•				•	•			•	•								•				•	•		
Healthcare data			•	•		•			•	•			•	•		•	•		•				•	•	•	•	•
Impact																											
Loss of availability	•	•			•	•	•	•			•	•				•		•		•	•	•		•	•		
Data integrity violation			•		•					•		•	•	•	•		•	•	•	•								•
Data confidentiality violation			•	•					•	•		•		•	•	•	•		•	•	•		•	•	•	•	•

Figure 7: Matrix of the Application Scenarios and the SPHINX Use Cases

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5 SPHINX Pilots Overview

This section introduces the set of pilots to be implemented in the SPHINX RIA, leveraging on the framework established by the SPHINX application scenarios and use cases. Aside from a first outline of the pilots' sites, a short presentation of the pilot activities to be performed is provided, with a specific attention to its specific benefits. In addition, it is also performed a preliminary approach to relevant Key Performance Indicators (KPIs) to consider with respect to which the performance of the SPHINX System will be ascertained.

Overall, the SPHINX Project encompasses 4 pilot sites:

- the General Hospital of Volos (GHV) supervised by the 5th Regional Health Authority of Thessaly & Sterea (DYPE5) in Greece;
- the University Hospital of Larissa (UHL) supervised by the 5th Regional Health Authority of Thessaly & Sterea (DYPE5) in Greece;
- the Polaris Medical Clinic (POLARIS) in Romania;
- the Hospital do Espírito Santo de Évora (HESE) in Portugal.

Three pilots will be conducted involving the 4 pilot sites, capturing the specifics of the SPHINX application scenarios and use cases. The planned SPHINX pilots are:

Pilots	Pilot Sites	Application Scenarios
Pilot in Greece: Intra-Region Patient Data Transfer	DYPE5 GHV; DYPE5 UHL	Sharing and Exchange of Healthcare Information
Cross-Border Pilot between Greece and Romania: Cross-border Medical Data Exchange	POLARIS; DYPE5	Cross-border Healthcare Service Delivery
Pilot in Portugal: Securing Advanced Patient Care in Hospital and Homecare Environments	HESE	mHealth and Remote Patient Monitoring

Table 60: SPHINX Pilots Overview

5.1 Description of SPHINX Pilot Sites

5.1.1 5th Regional Health Authority of Thessaly & Sterea (DYPE5)

The 5th Regional Health Authority of Thessaly and Sterea (DYPE5) is a Greek Public Sector's Authority that covers the mainland of Greece and is responsible for the uniform management, coordination, supervision and control of operations for all the healthcare and social services providers of Thessaly and Sterea providing health care services to approximately 2.000.000 population. The jurisdiction of the DYPE5 coincides with the administrative boundaries of the two districts. The entities that it supervises are listed below:

- 13 Hospitals;
- 33 Health Centres (primary healthcare provision);
- 321 peripheral surgeries (primary healthcare provision);
- 16 Urban Health Centres (primary healthcare provision).

Within the above context, the mission of 5th Regional Health Authority performs:

- The planning, coordination, supervision and control within the boundaries of the Health District concerned, of the operation of all Health Service Providers. The following are defined as Health Service Providers:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- Hospitals, Health Centers and Social Care Units;
- Mental Health and Addiction Centers;
- Other Public Law Entities and Public Private Law Entities, operating in the Health and Social Solidarity Sectors and supervised by the Minister of Health.

- The submission to the Ministry of Health of recommendations, measures and proposals aimed at providing efficient health services to the population of their Region;
- The monitoring the implementation by the Ministry of Health of the policy developed by the Ministry of Health.

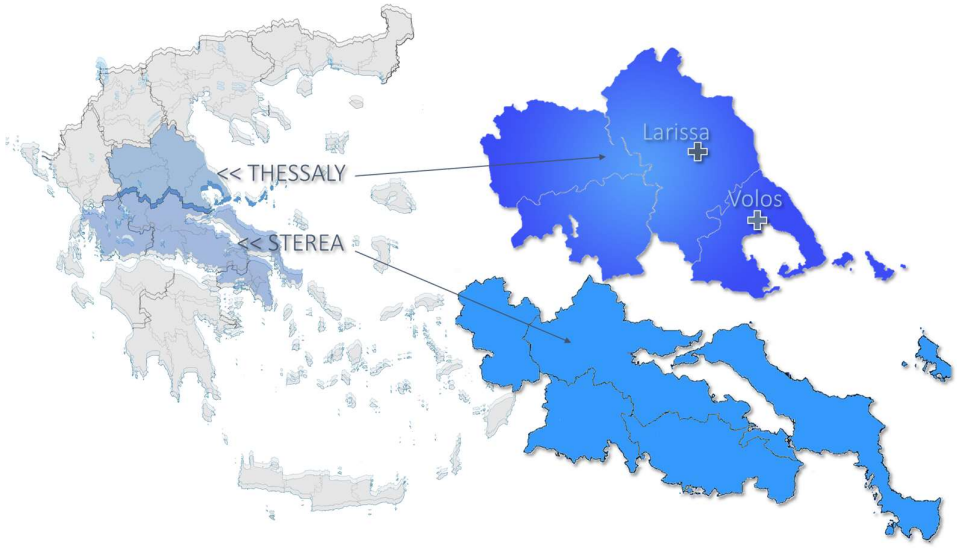

Figure 8: DYPE5's Area of Responsibility

Two pilot sites under the supervision of the 5th Regional Health Authority participate in SPHINX project i.e. the University Hospital of Larissa and the General Hospital of Volos. Both Hospitals are in the process of GDPR compliance.

5.1.1.1 University Hospital of Larissa

The University Hospital of Larissa was established in 1995 and started its operation in 1999. It is the largest provider of Health Services in the 5th Regional Health Authority with 650 beds. The purpose of the Hospital is to provide secondary and, above all, tertiary care to citizens through the operation of university clinics, laboratories in conjunction with special departments of the University of Thessaly School of Medicine, the training of physicians and other health and research scientists. It has 27 clinics, 9 specialist units, 24 clinics and 11 specialised laboratories and, with a staff of over 1,800 people it offers advanced, specialised services in internal medicine, cardiology, oncology, haematology, gastroenterology, endocrinology, paediatrics, neonatology, neurology, vascular surgery, thoracic surgery, thoracic surgery, thoracic surgery, thoracic surgery, among other specialties. The Hospital's annual turnover includes approximately 101,500 outpatients, 62,500 emergency and 61,000 patient admissions (2016 data). Its regular budget exceeds € 99,000,000 and the coverage of health care services covers over 2,000,000 people (Thessaly and Sterea - 2011 census). The information systems that are used in business process of the Hospital mainly comprise the hospital information systems (HIS), the laboratory information systems (LIS), the Pharmacy information system (PIS), Enterprise

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

resource planning (ERP). Medical Workstations coupled to associated Medical Devices are used to expedite patients' treatment plan. Building Management System is used to monitor building facilities (heating, air-cooling, oxygen supply) while UTM firewalls and relevant servers are used to monitor internet and local area network access. the University Hospital of Larissa is alternately on duty with the General Hospital of Larissa (the second hospital in Larissa County). Since 17th October 2019, the University Hospital of Larissa has been recognised as an Operator of Essential Services in the Greek Health Sector.

Figure 9: Aerial Photo of the University Hospital of Larissa

5.1.1.2 General Hospital of Volos

The *Achilopoulio* General Hospital of Volos with power of 400 beds, is on-call 24 hours a day, dealing with a large volume of chronic, emergency and emergency cases. The Hospital is divided into four sectors: a) Pathology Department with a capacity of 171 beds, b) Surgery Section with a capacity of 176 beds, c) Laboratory Section and d) Mental Health Section with a capacity of 40 beds. It started operating in 1903 and in 2007 it was moved to the new wing (total area of 40,000 sqm). It has about 800 staff covering the Magnesia prefecture with a population coverage of approximately 210,000 (2011 census), a figure that nearly doubles during the summer months. It operates 22 clinical and specialised units, 8 laboratories and the Hospital's annual turnover includes approximately 87,000 outpatients, 62,000 emergency and 23,000 patient admissions (2016 data). Its regular budget is EUR 37,000,000. Similarly, to the University Hospital of Larissa, the General Hospital of Volos utilises in its daily operation the hospital information systems (HIS), the laboratory information systems (LIS), the Pharmacy information system (PIS), Enterprise resource planning (ERP). Medical Workstations coupled to associated Medical Devices are used to expedite patients' treatment plan through digital imaging (DICOM) exchange. Building Management System is used to monitor building facilities (heating, air-cooling, oxygen supply) while UTM firewalls and relevant servers are used to monitor internet and local area network access.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Figure 10: Main Entrance of the General Hospital of Volos

5.1.2 Hospital do Espírito Santo de Évora (HESE)

The Hospital do Espírito Santo de Évora E.P.E. (HESE) is a public central hospital, serving the Alentejo region and integrated in the National Health Network.

Founded in 1495, with the name Real Hospital, HESE has undergone several changes, which explain the Hospital's large size and the dispersion of its physical structures. In fact, the Hospital is distributed by three buildings: the Edifício da Misericórdia, the Edifício do Espírito Santo and the Edifício Patrocínio. With more than 500 years, the convent-type building Edifício da Misericórdia is where the Administration, administrative services (human resources, financial services, legal cabinet, management planning and control, communication and marketing office, quality office, audit office) and support services (training cabinet, library, religious service, nutrition and dietetics, physical medicine and rehabilitation service, psychiatry and mental health and centralised sterilization service) are located. Coupled to the Misericórdia building, the Edifício do Espírito Santo has been inaugurated in 1975 to house the majority of internment services, namely Cardiology, Paediatrics, Orthopaedics, Ophthalmology, Otorhinolaryngology, General Surgery, Urology, Plastic Surgery, Paediatric Surgery, Obstetrics and Gynaecology, Medical Specialties, STROKE Unit, Digital Angiography Unit and Interventional Cardiology, General Urgency, Paediatric Urgency, intensive Care Unit, Neonatology, Pathological Anatomy and Pharmaceutics. In addition, this building also gathers the Health and Safety at Work, Facilities and Equipment and the Procurement services. Finally, the Edifício Patrocínio was built in 2001 and hosts the services of Medicine, Stoma, Medical Oncology, Immunohemotherapy, Radiotherapy, Haematology, Neurology, Immuno-allergology, Dermatology, External Consultations and Psychiatric internment, as well as Technology and Information Systems, Patient Management and Social Services. HESE is distinguished by its high level of technical differentiation in the clinical area, supported by modern technological equipment, and a team of highly qualified and motivated multidisciplinary professionals to provide the best healthcare to all users.

Currently, HESE has more than 1500 employees, including physicians, nurses, operational assistants, diagnostic and therapeutic technicians, administrative and support, and provides 314 hospital beds for an area serving directly 200 thousand habitants and indirectly about 300 thousand habitants. Indeed, Alentejo is the biggest region of Portugal (34% of Portugal's area) and most users live far from the hospital, benefiting from a very limited transport network.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Figure 11: HESE Area of Influence

In line with European guidelines, Portugal established its national strategy, the National Strategy for the Health Information Ecosystem (ENESIS 2020), that is essential for the success and improvement, in an exponential way, of public services provided to citizens. The Shared Services of Ministry in Health (SPMS), the entity responsible for Information Systems in Health, has been proactively leveraging the shift to digital transformation in the health system, based on the objective of improving the information quality and health care management, as well as increasing efficiency and technologically upgrade existing systems. Electronic Health Records answer to this priority in three ways: providing standardised solutions to health professionals use in healthcare setting (SONHO and SClínico), promoting healthcare continuity and clinical integration with primary care and continuity of care records, as well as for secondary use of data; allowing the registration and sharing of clinical information between citizens, health professionals and healthcare providers, including the private sector, complying with requirements of GDPR progressively; and allowing for cross-border sharing of patient summaries and ePrescription and eDispensation as off 2018. Portugal displays high adoption rates of specific eHealth services, namely the sharing of EHRs between departments, the picture archiving and communication system (PACS), ePrescription, integrated system for patient forwarding and the exchange of clinical care information with external suppliers.

As part of a modern hospital, HESE has a dedicated ICT Service that manages the daily operations of the hospital's informational infrastructure, a complex network of different types of equipment (medical equipment, computers, printers), various medical information systems (12) – accessing local and national patient medical databases –, numerous software applications dedicated to the hospital's management and administration procedures and activities and a large number of connected medical devices and health-related sensors. Examples of the medical information systems in HESE are SONHO (the System for Hospital and Primary Care Services), SINUS (the National System for Primary Care Services), GESTCARE CCI (the System for Registration and Monitoring of the National Network for Integrated Continued Care Services), PACS (the Picture Archiving and Communication System) and RNU (the National Registry of Patients). Overall, HESE dedicates significant attention to the security of its systems, data and infrastructure, implementing a number of best practices in the field concerning data privacy and user authentication, in compliance to applicable regulation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

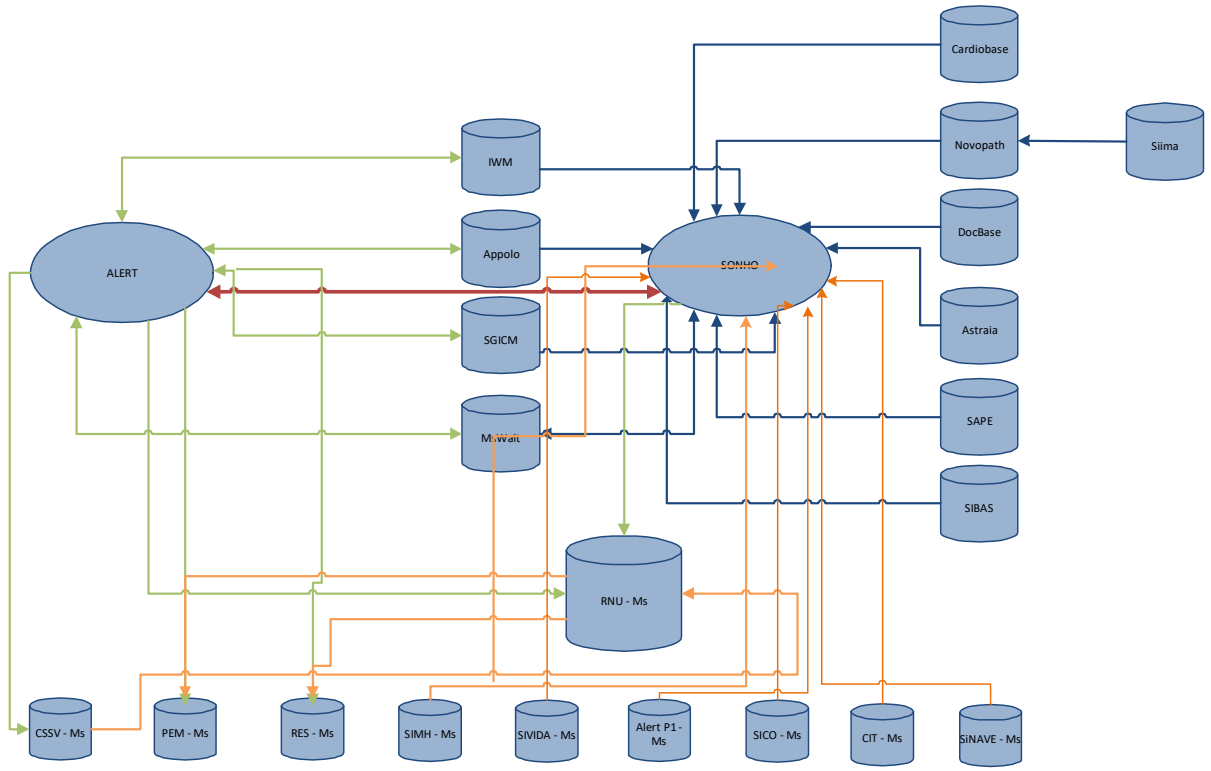

Figure 12: Diagram of the HESE Information Systems

Concerning the cybersecurity policies implemented at HESE, best practices are adopted with respect to security and to patients' privacy and personal data protection, in accordance to the General Data Protection Regulation (GDPR). From the cybersecurity perspective, HESE upholds restrictive access policies to the Hospital's network, involving the creation of new users, the connection of devices and the access to the Hospital's applications. HESE also provides open Internet access to guests via a wireless network that is isolated from the Hospital's network. Restrictive policies also apply to any remote connections to the Hospital's network and there is a proactive user account deactivation procedure. Further, all applications being connected to HESE's network are previously certified by the National Data Protection Authority.

5.1.3 POLARIS Medical Clinic [POLARIS]

The Polaris Medical Clinic is situated in a natural environment of 58000 square meters that allows patients to spend a great part of their time outdoors, whether enjoying ergo therapy activities, walking paths for recovery programs or simply a walk in the orchard.

Structured on five levels, the hospital has 180 beds for inpatient care, 14 beds for day care and ambulatory. Patients can be accommodated in wards with one, two or three beds, and each ward offers great comfort, being equipped with TV set and bathroom. The Polaris Clinic offers inpatient care services through the departments: Neurologic Rehabilitation, Cardiovascular Rehabilitation, Psychiatry, Physical Medicine and Rehabilitation and Palliative Care. The treatment base has a surface of over 700m, and includes a swimming pool, kinesiotherapy rooms, rooms for occupational therapy, rooms for physiotherapeutic and for massage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Figure 13: The Polaris Medical Clinic

The Polaris Medical Clinic's ICT infrastructure is built over HP and CISCO equipment. The LAN is built with multimode fiber optic links and cat 6 last mile using CISCO devices (LAN and core switches, firewall and routers). Medical devices, such as ultrasound, RX and CT scanners, are connected to the LAN. There is also a network of multifunctional printers used to scan and print medical documents. As part of the cybersecurity strategy, all computers in the Clinic (desktops, laptops, servers) has antivirus solutions installed and the routers are connected to the Internet behind a firewall (CISCO ASA). In addition, the Clinic has a building management system (BMS) in place to control the temperatures of every individual rooms, to control the access in hospital, and also a closed-circuit television (CCTV) system.

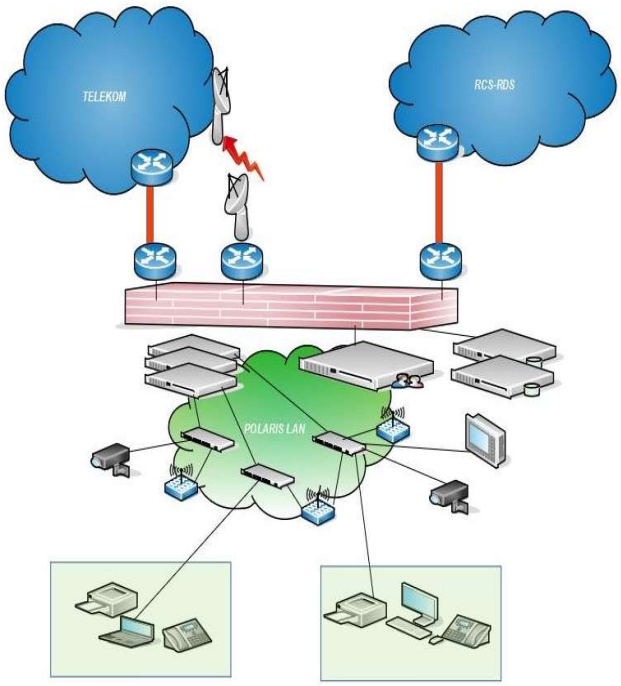

Figure 14: Diagram of the Polaris Medical Clinic Network

Concerning the cybersecurity policies implemented at the Polaris Medical Clinic, best practices are adopted with respect to security and to patients' privacy and personal data protection, in accordance to the General Data Protection Regulation (GDPR). From the cybersecurity perspective, the Clinic implements a restrictive access policy to the Clinic's network, involving the creation of new users (using Microsoft's Active Directory solution), the connection of devices and the access to the Clinic's applications. The Clinic also uses CISCO's VPN solution for remote connections to the Clinic's network.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5.2 The SPHINX Pilots

In the course of the SPHINX Project, three different pilot activities will unfold in Greece, Romania and Portugal.

5.2.1 Pilot in Greece: Intra-Region Patient Data Transfer

Considering the application scenario of **Sharing and Exchange of Healthcare Information**, the activities involving the "SPHINX Pilot in Greece: Intra-Region Patient Data Transfer" are built on the following SPHINX use cases:

- Use Case 04: Theft of Health Data by Exploiting Vulnerable Software;
- Use Case 06: Ransomware Attack to Healthcare Data;
- Use Case 12: Hacking Health IT Systems;
- Use Case 19: Illicit Rewriting of Patients' Medication;
- Use Case 25: Transfer of Patients Between Healthcare Organisations.

These use cases are fundamental to enable the development of specific test cases for the SPHINX pilots, to be elaborated as part of Task 7.3 – Real Life Scenario and Test Cases Definition.

In this pilot, involving the General Hospital of Volos (GHV) and the University Hospital of Larissa (UHL), both organisations within the region of the 5th Regional Health Authority (DYPE5), the intra-region scenario addresses the case of a patient hospitalised in the Cardiology clinic at the General Hospital of Volos that needs to be transferred to the University Hospital of Larissa in order to undergo a coronary angiography examination.

Once the patient arrives at the hospital in Larissa, the Medical Doctor requests the patient's health data (e-medical records) from the Hospital of Volos, that is:

- MRI and CT (DICOM data);
- Diagnosis (ICD-10 data);
- Medication received in Volos;
- Blood and Microbiological Lab test results.

Although both hospitals are based in the same region and utilise the same Hospital Information System inside SYZEFXIS, a private WAN network implementation, they operate as separate organisations under the Greek law in general, and the GDPR in particular, so they are not allowed to automatically share patient data between them. However, they are permitted to electronically share personal information of the patient through the use of the same HIS. Therefore, the HIS administrator of the Volos hospital needs to enable patient data read access rights for the University Hospital of Larissa. The process comprises the following steps, shown in **Figure 15**:

1) The Medical Doctor/Nursing/Administration Staff of Larissa Hospital contacts by phone/email the HIS administration of Volos asking for medical records of a specific patient that was transferred;
2) The IT department or relevant authorised HIS administration staff of Volos creates a temporary user name with a password in order to have access to GHV's HIS;
3) Case 1: A web link within the SYZEFXIS WAN secure network is sent via email to the UHL's Doctor followed by another separate email with username credentials. The password is revealed to the UHL doctor by telephone. The UHL's Doctor then has access to the HIS medical data of the Hospital of Volos;
4) Case 2: For robust purposes, in case the medical data (e.g. blood tests, DICOM data) are not available in the HIS database (this happens when doctors in GHV perform laboratory tests without ordering them via HIS due to emergency situation, so the results are only saved in the local LIS database), the GHV IT administrator gives access via RDP (the connection is established through the private WAN of SYZEFXIS)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

to a VM with LIS client & PACS client (e.g. radiant viewer) installed in order to see the requested data. If the UHL's Doctor wants to diagnose again the DICOM examinations, he can download the images through RDP into his computer and analyse them on a specific radiology workstation.

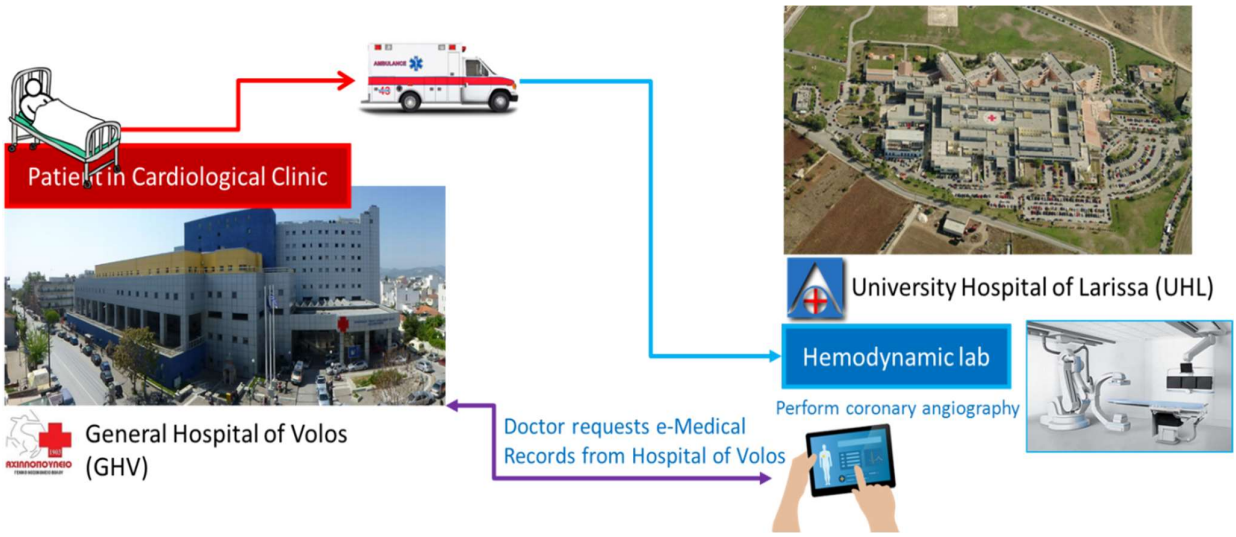

Figure 15: Intra-Region Pilot Schematics

As part of the SPHINX Pilot in Greece, the following activities will be conducted:

- Replication of the HIS and its database in a non-productive environment so as to emulate DYPE5's Hospitals operation during patient admissions;
- Deployment of a safe sandbox environment;
- Simulated patient data (medical diagnosis, medication, blood test results);
- Utilisation of the SPHINX toolbox to identify cyber vulnerabilities in the deployed environment and during data transmission between the two hospitals;
- Usage of SPHINX tools to neutralise or reduce cyber vulnerabilities during data-exchange and also in the HIS;
- Validation of the SPHINX toolkit's cyber security robustness and effectiveness against cyber threat vectors (conducted on a periodic basis).

Overall, the SPHINX Toolkit will establish user awareness of existing cyber threats, vulnerabilities and incidents, assure the security, integrity, availability, authenticity of the transmission of patients' data and generate stakeholders' (patients, hospital and medical teams) trust on the sharing and exchange of healthcare data. Specifically, the expected benefits of the SPHINX Pilot in Greece will be:

- Reinforcement of the Hospital's capability to securely interact with patients in intra-region data exchange;
- Reduction of the incidence of cyberattacks in both DYPE5's Hospitals;
- Improvement of security and privacy protection levels of highly sensitive patient data;
- Improvement of medical staff's and patients' trust in both in-hospital patient data exchange and also between hospitals, contributing to the time reduction of accessing patient data from other hospitals;
- Proposal of secure procedures assisted by the SPHINX toolkit during patient data exchange and communicate them to the associated policy-makers;
- Improvement of in-hospital cybersecurity capabilities;
- Provision of new-tools and cyber-security methodologies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5.2.2 Pilot in Greece and Romania: Cross-border Medical Data Exchange

Considering the application scenario of **Cross-border Healthcare Service Delivery**, the activities involving the "SPHINX Pilot in Greece and Romania: Cross-border Medical Data Exchange" are built on the following SPHINX use cases:

- Use Case 06: Ransomware Attack to Healthcare Data;
- Use Case 07: Distributed Denial-of-Service Attack in Regional Hospital;
- Use Case 16: Intercepting Cross-border Healthcare Data Exchange;
- Use Case 20: Compromised Workstation Allows the Scanning of Hospital Network;
- Use Case 26: Exploiting Medical Equipment to Steal Exams Results.

These use cases are fundamental to enable the development of specific test cases for the SPHINX pilots, to be elaborated as part of Task 7.3 - Real Life Scenario and Test Cases Definition.

In this pilot, involving the Polaris Medical Clinic (PMD) and a DYPE5 hospital, the cross-border scenario addresses the case of a Romanian tourist traveling to Greece which needs medical assistance at the DYPE5 hospital. The doctor from the DYPE5 hospital needs to check the patient's medical images, that is, CT scans (DICOM data) taken in the Polaris Medical.

The process comprises the following steps, displayed in Figure 16:

1) To gain access to the medical images, the DYPE5 doctor sends an e-mail to Polaris, requesting the documents;
2) After a brief check-up (DYPE5 doctor validation, Polaris doctor agreement), the imagery technician from Polaris sends an email with a link to the PACS images;
3) The DYPE5 doctor receives the email and accesses the link to the web interface of the PACS server to view the images from investigation.

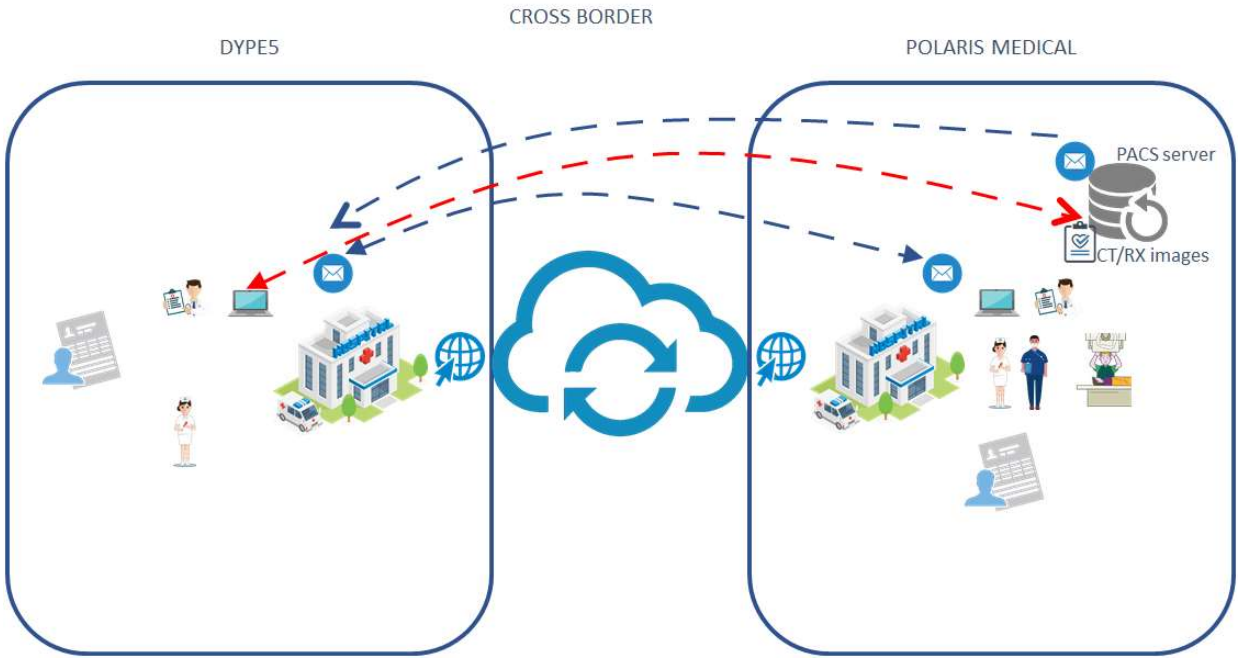

Figure 16: Cross-Border Pilot Schematics

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

As part of the SPHINX Cross-border Medical Data Exchange Pilot, the following activities will be conducted:

- Deployment of a safe sandbox environment, replicating the Polaris Medical Clinic's PACS server and email facilities, as well as the DYPE5 email server and HIS;
- Simulated patient data (DICOM data);
- Utilisation of the SPHINX toolbox to identify cyber vulnerabilities in the deployed environment and during data transmission between the Polaris Medical Clinic and the patient;
- Usage of SPHINX tools to neutralise or reduce cyber vulnerabilities during data exchange;
- Validation of the SPHINX toolkit's cyber security robustness and effectiveness against cyber threat vectors (conducted on a periodic basis).

Overall, the SPHINX Toolkit will establish user awareness of existing cyber threats, vulnerabilities and incidents, assure the security, integrity, availability, authenticity of the transmission of patients' data and generate stakeholders' (patients, hospital and medical teams) trust on the sharing and exchange of healthcare data. Specifically, the expected benefits of the SPHINX Cross-border Medical Data Exchange Pilot will be:

- Reinforcement of the capability of both Polaris Medical Clinic and DYPE5 hospital to securely interact for patient data exchange;
- Improvement of security and privacy protection levels of highly sensitive patient data in cross-border data exchange;
- Improvement of medical staff's and patients' trust in cross-border patient data exchange;
- Time efficient and secure access to patient data in cross-border environments;
- Improvement of overall organisational cybersecurity capabilities.

5.2.3 Pilot in Portugal: Securing Advanced Patient Care in Hospital and Homecare Environments

Considering the application scenario of **mHealth and Remote Patient Monitoring Platforms**, the activities involving the "SPHINX Pilot in Portugal: Securing Advanced Patient Care in Hospital and Homecare Environments" build on the following SPHINX use cases:

- Use Case 01: Attacking Obsolete Operating Systems in Hospital;
- Use Case 05: Tampering with Medical Devices;
- Use Case 10: Taking Control of Connected Medical Devices;
- Use Case 13: Exploiting Remote Patient Monitoring Services;
- Use Case 17: Accessing Health Data from a Fitness Tracker.

These use cases are fundamental to enable the development of specific test cases for the SPHINX pilots, to be elaborated as part of Task 7.3 – Real Life Scenario and Test Cases Definition.

The daily operations of Évora's Espírito Santo Hospital (HESE) are supported by different Information and Communications Technologies (ICT) for managing medical appointments, registering complementing diagnosis and therapeutics exams and accessing patient health records (the latter also accessible at the national level). HESE is currently testing the incorporation of modern medical and healthcare devices to support patient care to provide up-to-date information on patients' medical and health conditions.

With the purpose to improve patient care and recovery times while, at the same time, reduce costs and increase capacity of care, HESE and EDGE collaborate to remotely monitor on a 24/7 basis patients placed in homecare environments. To this end, HESE uses EDGE's eCare remote patient monitoring platform to integrate real-time data on patients' health parameters and activity gathered by various health devices, wearables and smart

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

assisted living sensors in hospital, medicalised residences and homecare environments. Using EDGE's eCare Platform, the Hospital's medic and nursing staff may consult remotely their patients' health condition and are alerted whenever worrisome signs are detected or imminent complications forecasted, delivering them the actionable intelligence to allow them to intervene timely upon critical patient information.

The eCare Platform used in the context of the collaboration between HESE and EDGE is illustrated in Figure 17.

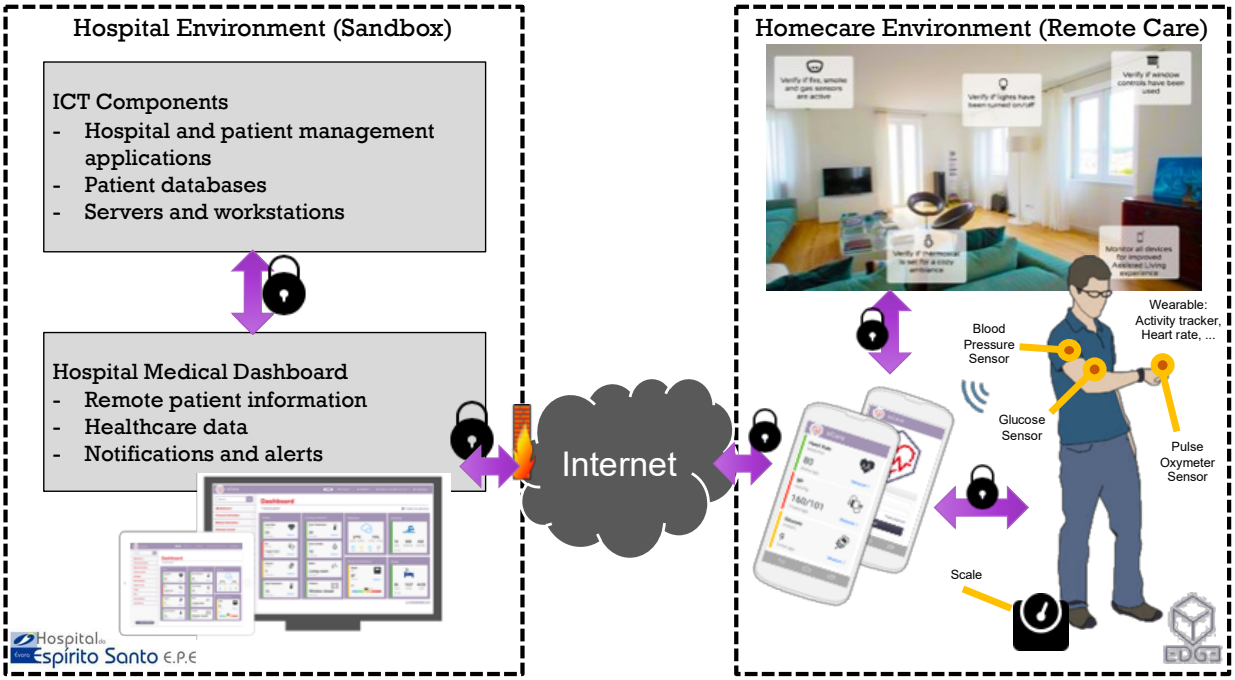

Figure 17: The mHealth and Remote Patient Monitoring Service at HESE

The integration of remotely connected health devices of the Remote Patient Monitoring Service with in-hospital ICT systems brings forth numerous challenges and concerns in what respects to patients' privacy, data protection, confidentiality and trust that need to be addressed. Importantly, the overall system's security and integrity needs to be ensured. While the hospital's environment is a well-controlled and secure environment, adopting best security policies, practices and processes and managed by well-trained and specialised staff, the patients' home environments are likely handled by non-experts, even technology illiterate users, and scarce of best security practices. Thus, the remote patient homecare environment introduces new challenges and potential threats to the Hospital's ICT infrastructure that need to be specifically addressed.

In this context, the SPHINX Pilot in Portugal aims to the demonstrate and validate the SPHINX toolkit in delivering a highly secure system against cyber threats, considering patient care in hospital and homecare settings.

In SPHINX, a safe sandbox environment will be created, consisting of a realistic or close-to-real environment that replicates the mHealth and Remote Patient Monitoring Service enabled by the eCare Platform. EDGE's eCare components and devices will be adapted to implement the SPHINX tools. In addition, the SPHINX Pilot in Portugal will be demonstrated in three simulated remote care environments.

As part of the SPHINX Pilot in Portugal, the following activities will be conducted:

- Deployment of a safe sandbox environment, replicating the eCare setup deployed by HESE and EDGE,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

involving workstations, software applications, databases and connected health and smart home devices;
- Deployment of simulated remote care environments (no real data involved), including data generated by smart health devices (e.g., blood pressure, heart rate and blood glucose sensors and smart scales) and smart home devices (e.g., ambient quality sensors);
- Utilisation of the SPHINX toolbox to identify cyber vulnerabilities in the deployed environment;
- Incorporation and implementation of SPHINX tools to neutralise or reduce cyber vulnerabilities in the deployed environment;
- Validation of the SPHINX toolkit's cyber security robustness and effectiveness against cyber threat vectors (conducted on a periodic basis).

Overall, the SPHINX Toolkit will establish user awareness of existing cyber threats, vulnerabilities and incidents, assure the security, integrity, availability, authenticity of the transmission of patients' data and generate stakeholders' (patients, hospital and medical teams) trust on the delivery of mHealth and Remote Patient Monitoring services. Specifically, the expected benefits of the SPHINX Pilot in Portugal will be:

- Reinforcement of the Hospital's capability to securely interact with patients in remote care settings;
- Reduction of the incidence of cyberattacks in HESE, namely those associated with remote care settings;
- Delivery of a secure remote monitoring system;
- Improvement of security and privacy protection levels of highly sensitive patient data;
- Improvement of medical staff's and patients' trust in remote patient monitoring solutions, contributing to an improved patient's quality of life and the reduction of healthcare costs;
- Improvement of cybersecurity capabilities for small and medium businesses, enabling market uptake of innovative mHealth and remote patient monitoring solutions.

5.3 Key Performance Indicators for SPHINX Pilots

A key performance indicator (KPI) can be defined as an item of information collected at regular intervals to track the performance of a system [20]. In other words, it can be used to monitor and measure a system's effectiveness or lack of thereof. KPIs are typically linked to high-level goals and are used to drive strategic and tactical decisions. They can also be used to provide actionable insights supporting decision-making and driving continuous improvement. Given that there is an associated cost in implementing KPIs - either in measuring or assessing -, it is important to perform a careful selection of KPIs, ensuring these capture critical performance aspects of the system.

As recommended in [21], the KPIs selection should be valued above quantity. KPIs should therefore be defined following the well-known SMART principle:

- **Simple** – KPIs should not be overly complicated to measure. It should be clear what the purpose of each KPI is and how it impacts the system;
- **Measurable** – A KPI must be able to be measured in some way, quantitatively or qualitatively. The method by which each KPI is measured should be clearly defined and consistent;
- **Actionable** – KPIs should be used as a driver for decisions. The purpose of a KPI is to measure performance, and if necessary, take some action based on the results;
- **Relevant** – Each KPI should be a measurement of the function being assessed;
- **Time Based** – KPIs can and should be used to show changes over time. An effective KPI should be able to be collected and grouped by various time intervals to show variations and patterns.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

When considering the definition of KPIs, it is possible to identify the following strategic goals for the SPHINX System:

- **GOAL 1: Technical Effectiveness** - the SPHINX System will be able to forecast, predict and detect all cybersecurity incidents;
- **GOAL 2: Reliability, Availability and Maintainability** - the SPHINX System will exhibit highly consistent and accurate results, high availability and easy maintenance capabilities.
- **GOAL 3: Automation** - the SPHINX System will operate with a high degree of automation, requiring little to no operator intervention.
- **GOAL 4: Usability** - the SPHINX System will be easy to use, via an intuitive interface (simple but comprehensive) that enables operators to rapidly develop awareness concerning cyber security incidents and suspicious cybersecurity events. SPHINX will aim to obtain a high level of user acceptance;
- **GOAL 5: Cybersecurity Awareness and Behaviour** - the SPHINX System will contribute to improve cybersecurity awareness and behaviour prone to the adoption of cybersecurity best practices.
- **GOAL 6: User Adoption** - the SPHINX System will be trusted by users, contributing to its adoption.

In SPHINX, abiding to the SMART principle, several KPIs have been defined to adequately assess the effectiveness of the SPHINX System's critical functions as they strive to realise the proposed strategic goals.

Identifier	SPHINX KPIs	Description
KPI 1	Detection of Cybersecurity Events	Assessment of the number of cybersecurity events detected or identified by SPHINX.
KPI 2	Resolution of Cybersecurity Events	Assessment of the time spent by SPHINX in the resolution of detected cybersecurity events.
KPI 3	Impact of Cybersecurity Events	Assessment of the impact of cybersecurity events detected or identified by SPHINX.
KPI 4	SPHINX Reliability, Availability and Availability	Assessment of the consistency of the SPHINX performance, the continuous access to the SPHINX system and the easiness to conduct upgrades and maintenance operations in the SPHINX system.
KPI 5	SPHINX Automation	Assessment of the automation level and the automation effectiveness of SPHINX's critical functions.
KPI 6	User Satisfaction	Assessment of the users' perception of SPHINX's performance and operational efficiency, including the assessment of the user's fatigue while operating SPHINX.
KPI 7	Cybersecurity Awareness and Behaviour	Assessment of the SPHINX impact in users' cybersecurity awareness and behaviour.
KPI 8	Trust and Adoption of SPHINX	Assessment of the users' trust in the SPHINX System and the health digital services, as well as their willingness to adopt and use the SPHINX System and the health digital services.

Table 61: Key Performance Indicators for the SPHINX System

Aside from being useful to assist organisations throughout the implementation process of the SPHINX System, the SPHINX KPIs will be selected and operationalised (in association with specific success measures) to support the assessment of the SPHINX System in the three SPHINX Pilots. Consequently, it is noted that the SPHINX KPIs will be finalised within the activities performed in Work Package 7.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

KPIs for the SPHINX Pilots		Measure	Assessed Variable	Success Measure
Technical Effectiveness				
KPI 1	Detection of Cybersecurity Events			
KPI 1.1	Number of predicted threats	# events/week	Risk, User workload	DPP[6]
KPI 1.2	Number of forecasted threats	# events/week	Risk, User workload	DPP
KPI 1.3	Number of detected cyber vulnerabilities	# events/week	Risk, User workload	DPP
KPI 1.4	Number of detected unauthorised BYOD accesses	# events/week	Risk, User workload	DPP
KPI 1.5	Number of registered security incidents	# events/week	Risk, User workload	DPP
KPI 1.6	Number of registered abnormal events	# events/week	Risk, User workload	DPP
KPI 1.7	Number of unauthorised accesses to medical devices	# events/week	Risk, User workload	DPP
KPI 2	Resolution of Cybersecurity Events			
KPI 2.1	Total time to detect	minutes	Efficiency	< 1
KPI 2.2	Total time to resolve	hours	Efficiency	< 1
KPI 2.3	Service response latency	seconds	Efficiency	< 5
KPI 2.4	Service recovery after cyber-attack	hours	Efficiency	< 1
KPI 3	Impact of Cybersecurity Events			
KPI 3.1	Incident impact per incident	Ordinal scale (1-5)[7]	Liability risk	DPP
Reliability, Availability and Maintainability				
KPI 4	SPHINX Reliability, Availability and Maintainability			
KPI 4.1	Consistency of results	%	Reliability	> 95%
KPI 4.2	Service availability	%	Availability	> 95%
KPI 4.3	Total time to maintain the system	hours	Maintainability	< 1
KPI 4.4	Total time to update the system	hours	Maintainability	< 1
Automation				
KPI 5	SPHINX Automation			
KPI 5.1	Automation level of security processes	Ordinal scale (1-5)[8]	User workload	4 or higher
KPI 5.2	Automation effectiveness of security processes	Ordinal scale (1-5)[5]	User workload	4 or higher
Usability				
KPI 6	User Satisfaction			
KPI 6.1	Intuitive presentation	Ordinal scale (1-5)[9]	User acceptance	4 or higher
KPI 6.2	Friendly dashboard	Ordinal scale (1-5)[6]	User acceptance	4 or higher

[6] Defined per pilot within deliverable D7.5.

[7] Ordinal scale: 1 - Very low (no serious disruption of services, no breach of user/patient data); 2 - Low (local disruption to non-critical services, no breach of user/patient data); 3 - Moderate (non-critical service availability affected, likely breach of user/patient data); 4 - High (critical service availability affected, breach of user/patient sensitive data); 5 - Very High (no services available, breach of user/patient sensitive data).

[8] Ordinal scale: 1 - Manual; 2 - Assisted (Low level of automation); 3 - Semi-Automated; 4 - Highly automated; 5 - Fully automated [22].

[9] Ordinal scale: 1 - Very low; 2 - Low; 3 - Neutral; 4 - High; 5 - Very High.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

KPIs for the SPHINX Pilots		Measure	Assessed Variable	Success Measure
KPI 6.3	Easy-to-use navigation	Ordinal scale (1-5)[6]	User acceptance	4 or higher
KPI 6.4	Time for task completion	Ordinal scale (1-5)[6]	User acceptance	4 or higher
KPI 6.5	Duration of task	Ordinal scale (1-5)[6]	User acceptance	4 or higher
KPI 6.6	Error rate in task execution	Ordinal scale (1-5)[6]	User acceptance	4 or higher
KPI 6.7	User fatigue	%	User acceptance	< 5%
Cybersecurity Awareness and Behaviour				
KPI 7	Cybersecurity Awareness and Behaviour			
KPI 7.1	Knowledge of cybersecurity best practices	# cybersecurity best practices	Security culture	> 5
KPI 7.2	Adoption of cybersecurity behaviours	# behavioural changes	Security culture	> 2
KPI 8	Trust and Adoption of SPHINX			
KPI 8.1	Trust in the SPHINX System	Ordinal scale (1-5)[6]	Security culture	4 or higher
KPI 8.2	Increased trust in eHealth and mHealth services and medical devices	Ordinal scale (1-5)[6]	Security culture	4 or higher
KPI 8.3	Adoption of the SPHINX System	Ordinal scale (1-5)[6]	Security culture	4 or higher
KPI 8.4	Increased use of eHealth and mHealth services and medical devices	Ordinal scale (1-5)[6]	Security culture	4 or higher

Table 62: Key Performance Indicators and Success Measures for the SPHINX Pilots

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

6 Conclusion

This report constitutes the final result of Task 2.4 – Reference Scenarios, Pilot Operations and KPIs in the SPHINX Action and presents the five application scenarios and a set of twenty-seven use cases developed for SPHINX. The SPHINX use cases may be used by healthcare organisations in cybersecurity preparation and planning, as well as for education awareness, training activities and the validation of the SPHINX System.

The initial set of twenty-one SPHINX use cases has been updated, with the refinement of use cases to better align with the ongoing development, testing and integration activities involving the SPHINX tools, detailing those tools' intervention, as well as with the generation of six new use cases deemed of relevance to healthcare organisations and covering a panoply of cybersecurity incidents and attacks in which the use of SPHINX's unique features does make a difference.

The selected use cases are inspired either by real cybersecurity incidents or by public information (literature) and benefit from the extensive experience of the SPHINX end-user partners. All the information provided in the use cases' descriptions are solely based on open source information and the use cases are purposefully kept generic and general, but with sufficient detail to be useful for adaptation and subsequent extrapolation. The intention is that these use cases can be adjusted and specified in more detail dependent upon the specific purpose. For instance, in the SPHINX pilots, the use cases form the basis for the storyline development.

In addition, this document provides a brief overview of the three SPHINX pilot sites and of their planned piloting activities aiming to assess the performance of the SPHINX System in the face of cybersecurity events, incidents and attacks. To facilitate the SPHINX assessment effort, eight KPIs have been identified by the SPHINX partners and are in the present document detailed into measures, assessed variables and success measures to better frame the evaluation analysis to be performed within Work Package 7, in order to ascertain SPHINX's positive impact and benefits as part of the cybersecurity protection tools adopted and operated by healthcare organisations to deal with the growing cybersecurity challenges of today and tomorrow.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

7 References

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*. September 2012. Version 3.1, Revision 4.
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*. September 2012. Version 3.1, Revision 4.
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*. September 2012. Version 3.1, Revision 4.
4. *ENISA Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures*. European Union Agency for Network and Information Security. November 2016.
5. *ENISA Security and Resilience in eHealth - Security Challenges and Risks*. European Union Agency for Network and Information Security. 2015
6. *ENISA Reference Incident Classification Taxonomy - Task Force Status and Way Forward*. European Union Agency for Network and Information Security. January 2018.
7. https://github.com/MISP/misp-taxonomies.
8. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology/ontology_taxonomies.
9. https://www.csoonline.com/article/3203804/know-your-enemy-understanding-threat-actors.html.
10. https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/threats-attacks-and-vulnerabilities-in-security/how-to-explain-threat-actor-types-and-attributes/#gref.
11. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.
12. *Data Breach Investigations Report*. Verizon Enterprise. 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.
13. *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. Ponemon Institute. 2016. https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf.
14. *Accenture 2018 Healthcare Workforce Survey on Cybersecurity*. Accenture. YouTube. 2018. https://www.youtube.com/watch?v=1WI_o7VQQxI.
15. Gavin O'Brien et. al. Securing Electronic Health Records on Mobile Devices. National Institute of Standards and Technology. July 2018. https://doi.org/10.6028/NIST.SP.1800-1.
16. The Internet of Things 2019. Peter Newman. Business Insider Intelligence. January 2019.
17. *Unlocking the potential of the Internet of Things*. James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. McKinsey Global Institute. June 2015.
18. *19 million will use remote patient monitoring by 2018*. MEDCITY News. http://medcitynews.com/2014/06/biggest-market-remote-patient-monitoring/.
19. Conficker Working Group. *Lessons Learned*. June 2010. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

20. Carol Taylor Fitz-Gibbon (1990). *Performance indicators*. BERA Dialogues. ISBN 978-1-85359-092-4.

21. John Moran. *Key Performance Indicators (KPIs) for Security Operations and Incident Response*. DFLABS. https://www.dflabs.com/wp-content/uploads/2018/03/KPIs_for_Security_Operations_and_Incident_Response-2.pdf.

22. Frank Flemisch, Matthias Heesen, Tobias Hesse, Johann Kelsch, Anna Schieben and Johannes Beller. 2012. *Towards a dynamic balance between humans and automation: authority, ability, responsibility and control in shared and cooperative control situations*. Cognition, Technology & Work. March 2012, Volume 14, Issue 1, pp 3–18. https://doi.org/10.1007/s10111-011-0191-6.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.