D7.1 Pilot plans including evaluation framework

WP7 – Technology Validation Pilots and Privacy Assessment

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	Reza RAZAVI (CNECT/H/03)			
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA			
Deliverable	D7.1 - Pilot plans including evaluation framework			
Work Package	WP7 - Technology Validation Pilots and Privacy Assessment			
Date of Delivery	Contractual	M18	Actual	M18
Nature	R - Report	**Dissemination Level**	P - Public	
Lead Beneficiary	HESE			
Responsible Authors	Ricardo Cabecinha	Email	rjcabecinha@hevora.min-saude.pt	
		Phone	-	
	Fotios Gioulekas	Email	fogi@dypethessaly.gr	
		Phone	-	
Reviewer(s):	ICOM; HMU			
Keywords	Surveys on Cybersecurity Awareness, ICT Infrastructure at Pilot Sites, Planning of Pilot Operations, SPHINX Pilots' Evaluation 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.

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	01/07/2019	Draft	ToC	Ricardo Cabecinha (HESE)
0.20	03/07/2019	Draft	Content Creation	Ricardo Cabecinha (HESE), Fotios Gioulekas, Vagelis Stamatiadis, Athanasios Tzikas, Konstantinos Gounaris (DYPE5), Dana Oniga (SIMAVI), Sergiu Marin (POLARIS), Marco Manso and Bárbara Guerra(EDGE)
0.30	07/10/2019	Draft	Internal Review 1	Fotios Gioulekas, Vagelis Stamatiadis, Athanasios Tzikas, Konstantinos Gounaris (DYPE5)
0.40	07/05/2020	Draft	Content Consolidation	Ricardo Cabecinha (HESE), Fotios Gioulekas, Vagelis Stamatiadis, Athanasios Tzikas, Konstantinos Gounaris (DYPE5), Sergiu Marin (POLARIS), Marco Manso and Bárbara Guerra(EDGE), Dana Oniga (SIMAVI)
0.50	28/05/2020	Draft	Internal Review 2	Marco Manso, Bárbara Guerra, José Pires (EDGE)
0.60	18/06/2020	Draft	Review 1	Yannis Nikoloudakis (HMU)
0.70	19/06/2020	Draft	Review 2	Illias Lamprinos (ICOM)
0.80	22/06/2020	Pre-final	Update to reflect the reviewers' comments	Ricardo Cabecinha (HESE)
0.90	24/06/2020	Pre-final	Quality Control	George Doukas (NTUA), Michael Kontoulis (NTUA)
1.00	25/06/2020	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 deliverable reports the work carried out in Task 7.1 - Sites Surveys and Planning of Pilot Operations. It presents the results of the regular reviews performed on all pilot sites in terms of their characteristics, operations and settings that affect the deployment and operation of the SPHINX Toolkit. Specifically, this document establishes the baseline of the cybersecurity awareness level at each of the SPHINX pilot sites, involving both the staff of the Information and Communication Technology (ICT) departments and the remaining professionals working at the pilot sites. Additionally, the ICT infrastructure of the pilot sites is described, as well as its critical assets associated to prevailing business processes and daily operations, requiring protection. Furthermore, this document reviews the roles, responsibilities, organisational structures, assets, security processes and logistics processes across all the pilot sites. It catalogues the information needed from each pilot site for the deployment and operation of the SPHINX Toolkit. Finally, this report delineates a detailed planning of the proposed pilot operations, in terms of the activities to be implemented, the timing of these activities and the evaluation framework created to assess and validate the SPHINX Toolkit's performance and added-value for the healthcare organisations' cybersecurity operations. It is worth noting that elements in this document have been submitted for the Elsevier publication "*Healthcare: The Journal of Delivery Science and Innovation*" on June 16th, 2020.

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 Abbreviations

ABS – Attack and Behaviour Simulators

AD – Anomaly Detection

AE – Analytic Engine

AI – Artificial Intelligence

AP – Anonymisation and Privacy

BBTR – Blockchain Based Threats Registry

BMS – Building Management System

BYOD – Bring Your Own Device

CCTV – Closed Circuit Television

CSIRT – Computer Security Incident Response Team

CST – Cyber Security Toolbox

CT – Computed Tomography

DDOS – Distributed Denial of Service

DSS – Decision Support System

DTM – Data Traffic Monitoring

ECG – Electrocardiogram

ENISA – European Union Agency for Cybersecurity

ERP – Enterprise Resource Planning

EU – European Union

FDCE – Forensic Data Collection Engine

GDPR – General Data Protection Regulation

HE – Homomorphic Encryption

HIS – Hospital Information System

HP – Honeypot

ICT – Information and Communication Technology

ID – Interactive Dashboards

IoMT – Internet of Medical Things

IoT – Internet of Things

IT – Information Technology

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.

KB – Knowledge Base

KPI – Key Performance Indicator

LIS – Laboratory Information System

MLID – Machine Learning-empowered Intrusion Detection

MRI – Magnetic Resonance Imaging

NAS – Network Attached Storage

PACS – Picture Archiving and Communication System

PDA – Personal Digital Assistant

PIS – Pharmacy Information System

QoS – Quality of Service

RCRA – Real-time Cyber Risk Assessment

RDP – Remote Desktop Protocol

RFID – Radio-Frequency IDentification

SIEM – Security Information and Event Management

SMART – Specific, Measurable, Attainable, Realistic and Timely

SMS – Short Messaging Service

SPA – Security Protocol Analysis

UTM – Unified Threat Management

VAaaS – Vulnerability Assessment as a Service

VLAN – Virtual Local Area Network

VM – Virtual Machine

VPN – Virtual Private Network

WAN – Wide Area Network

WP – Work Package

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 and Scope

This document, *D7.1 - Pilot Plans Including Evaluation Framework*, is elaborated as part of Task 7.1 - Sites Surveys and Planning of Pilot Operations and presents the SPHINX detailed planning of pilot operations. The pilot operations plan describes the activities to be performed, the roles, responsibilities, organisational structures, assets, security processes and logistics processes in all the four pilot sites, as well as the evaluation framework to be applied for the assessment and validation of the SPHINX Toolkit.

Healthcare organisations (e.g., hospitals, care centres) from different countries became targets of cyber-attacks (e.g. data theft, denial-of-service, ransomware) due to the high value of health records in the black market and the growth of the attack surface of those healthcare organisations due to the introduction of the digitisation of processes, eHealth and mHealth technologies, the Internet of Medical Things (IoMT) and the need to exchange healthcare data among healthcare organisations to support healthcare delivery.

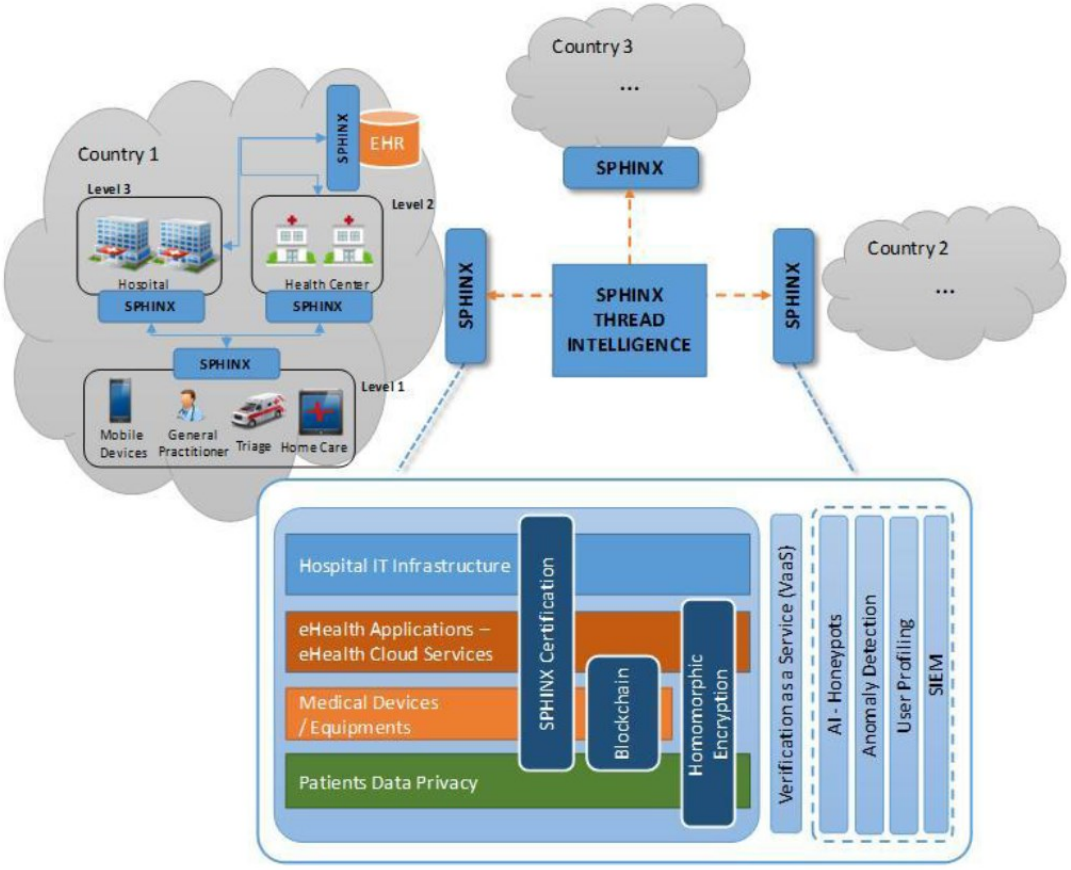

Figure 1: Description of the SPHINX Concept

As shown in Figure 1, the SPHINX Toolkit will deliver advanced cybersecurity protection to four healthcare organisations, acting as reference pilot sites in three countries: Greece, Romania and Portugal.

The SPHINX pilots will test and validate the SPHINX Toolkit in realistic conditions, leveraging the reference scenarios and use cases defined in WP2 - Conceptualisation, Use Cases and System Architecture, *D2.4 - Use Cases Definition and Requirements Document v1* [1].

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 Toolkit protects the exchange of medical data between healthcare providers through its components and improves cyber protection of the infrastructure of healthcare organisations. It also ensures the patients' data privacy and integrity, by identifying modern and advanced cyber threats and by preventing or reducing the occurrence of cyber-attacks.

According to deliverable *D2.6 - SPHINX Architecture v2* [2], the major building blocks that comprise the SPHINX Toolkit and its advanced cybersecurity capabilities for the healthcare sector are the Device Verification and Certification, the Automated Cyber Security Risk Assessment, the Decision Support System and Interactive Dashboards, the Cyber Security Toolbox, the Third-party APIs and the Common Integration Platform. Specific SPHINX tools will be dedicated to specific elements of the ICT ecosystem, such as protocol analysis, detection of anomalous behaviour, security events, intrusion detection, vulnerability assessment and honeypots. Through the Common Integration Platform, the SPHINX Toolkit enables each SPHINX tool to be deployed independently and enables the interaction of third-party healthcare solution providers with SPHINX's tools.

SPHINX users are able to interact with the multiple services and functions of the SPHINX Toolkit in an intuitive and user-friendly way, through Interactive Dashboards. In the Interactive Dashboard, users receive alerts about cyber security threats or attacks and associated reports, containing recommendations on appropriate response actions following a detected cyber-attack and where the cyber-attack happened. Aside from the interactive dashboard, the SPHINX Toolkit provides a personalised data security management tool that allows users to setup the tools required by the ICT ecosystem. The SPHINX Toolkit even allows users to run and validate simulated application scenarios and use cases in a safe and isolated testing environment.

1.2 Structure of the Deliverable

This document is structured as follows: Section 1 introduces the document; Section 2 presents the results of the questionnaires on the cybersecurity awareness levels at the pilot sites; Section 3 presents the assets and the ICT infrastructure of the healthcare organisations involved in the pilots (e.g., remote assets, network medical devices, mobile client devices); Section 4 details each pilot activity, describing the actions to be performed, the involved partners and the pilots' evaluation framework; Section 5 summarises the planning of the SPHINX pilot operations; and finally, Section 6 concludes the document.

1.3 Relation to other WPs & Tasks

This report benefits from the work performed in most of SPHINX Work Packages:

- WP2: Conceptualisation, Use Cases and System Architecture;
- WP3: Cybersecurity Risk Assessment & Beyond – SPHINX Intelligence;
- WP4: SPHINX Toolkits;
- WP5: Analysis and Decision Making;
- WP6: SPHINX Common Integration Platform & Incremental Strategy.

The application scenarios, use cases and high-level description of the SPHINX pilots in deliverable *D2.4 - Use Cases Definition and Requirements Document v1* [1] are relevant for the testing and validation of the SPHINX Toolkit in realistic conditions to establish its performance and contribution to the assessment of cyber threats and the prevention of cyber-attacks in healthcare organisations. Similarly, the functional and non-functional requirements and the guidelines described in deliverable *D2.5 - SPHINX Requirements and Guidelines v1* [3] have assisted in the detailed design and planning of the pilot activities.

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.

Work Packages 3, 4, 5 and 6 are responsible for the development and integration of the SPHINX tools, designed and implemented using the architecture and technical specifications included in deliverable *D2.6 - SPHINX Architecture v2* [2]. Those tools will be validated in the SPHINX pilots to determine the extent of the benefits brought by the SPHINX system to the healthcare sector.

In addition, the work performed in Task 7.1: Sites Surveys and Planning of Pilot Operations, summarised in this document, provides relevant information for the effort devoted in WP7, leading to the production of deliverables *D7.4 - SPHINX Ecosystem Demo Platform* and *D7.5 - Real-life Pilot Demonstrators Results and Consolidation Including Stakeholders Experience Evaluation and Cost Assessment*.

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 The Cybersecurity Awareness Status of Pilot Sites

WP7 is dedicated to the validation of the SPHINX Toolkit via the execution of pilot activities in four pilot sites in Greece, Romania and Portugal. The activities in this Work Package started with an effort to establish the level of cybersecurity awareness at the healthcare organisations acting as pilot sites, involving not only the ICT department teams but also the different types of professionals working in those organisations, before the deployment of the SPHINX Toolkit. The objective is to first establish a baseline and then to adequately evaluate the cybersecurity awareness status of the pilot sites before and after the SPHINX deployment.

2.1 Survey Design and Methodology

According to the 2018 statistics on the proportion of ICT specialists in total employment published by Eurostat [4], it is observed that the relevant percentage for Portugal, Romania and Greece (the countries hosting the SPHINX pilots) is significantly below the EU-28 average percentage, as illustrated in Figure 2.

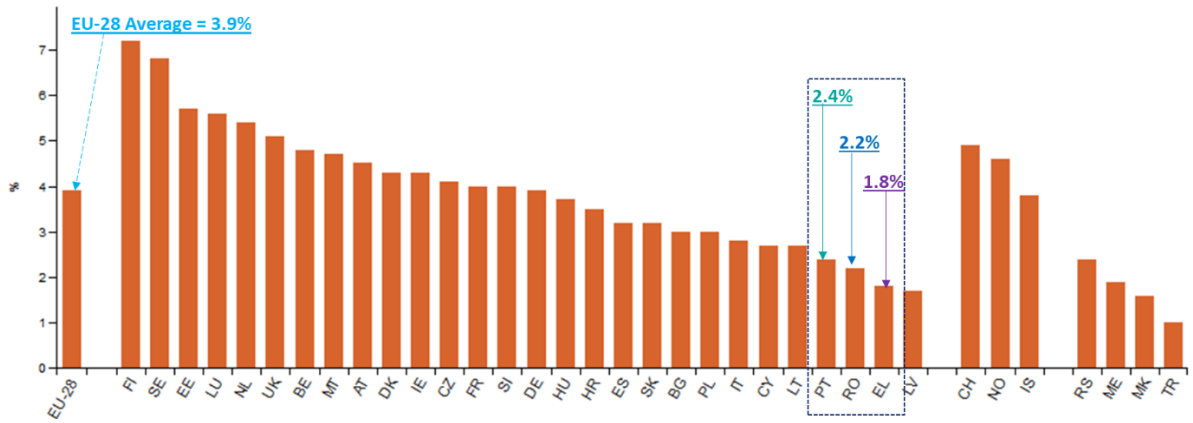

Figure 2: Proportion of ICT Specialists in Total Employment

Taking into account the aforementioned report, it is the SPHINX partners' objective to establish the level of cybersecurity awareness in the healthcare organisations involved in the SPHINX pilots and to explore whether the limitation in ICT employment and resources, in general, could potentially affect the vulnerability of those organisations to cybersecurity-related threats. To this end, two surveys were created: the first targeted to the ICT departments and the second one is focused on the non-ICT employees (medical, auxiliary, laboratory and administrative personnel).

The ICT questionnaires present five parts: the first part refers to demographics (i.e. years of experience, served population, type of healthcare organisation and total number of employees); the second part deals with questions related to ICT daily activities, such as the number of performed cybersecurity trainings, the cybersecurity budget allocation, the ICT percentage employment and the presence of Cybersecurity departments; the third section focuses on the employed login and networking policies and users' external accesses; the fourth section includes questions on existing cybersecurity practices; and the fifth section contains questions security incidents and the *time to respond*. On the other hand, the non-ICT questionnaire comprises questions on demographics, status of the employment, performed training on the General Data Protection Regulation (GDPR), the capacity to identify cyberattacks and the familiarity with security processes and precautions.

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.

Tables 1 and 2 present the questions included in the two questionnaires.

1. General Characteristics

a. Demographics

i. Age

20-39 ☐ 40-60 ☐ 60+ ☐

ii. Gender

Male ☐ Female ☐

iii. Education

Secondary Education ☐ Vocational training Institution ☐

Bachelor Degree ☐ MSc ☐ PhD ☐

iv. Position

ICT director ☐ ICT manager ☐ ICT staff ☐

v. Years of experience

0-5 ☐ 6-10 ☐ more than 10 ☐

vi. Healthcare Organisation

Hospital ☐ Clinic ☐ Health Authority ☐

National ☐ Regional ☐ Local ☐

Employees <100 ☐ Employees 100-300 ☐ Employees 301-600 ☐

Employees 601-1000 ☐ Employees >1000 ☐

Population <100k ☐ Population 100k-300k ☐ Population >300k ☐

2. Specific ICT

a. Proportion of ICT employees in total employment (%)

0-1% ☐ 1.1-2% ☐ 2.1-3%☐ 3.1-4% ☐ 4.1-5% ☐ 5.1-6% ☐ 6.1-7% ☐

b. Existence of a Cyber-Security Department

Yes ☐ No ☐

c. Official Trainings had in ICT Cyber Security during the last 3 years (number)

0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐

d. Do you perform internal cybersecurity awareness trainings (e.g. phishing) in order to teach employees what to check in the received emails?

Yes ☐ No ☐

e. Average Yearly Organization's budget allocated to ICT during the last 3 years (in Euros)

0-100K ☐ 101K-200K ☐ 201K-300K ☐ 301K-400K ☐ 401K-500K ☐

Do not know ☐

f. Percentage of Current ICT Budget Allocated to Cybersecurity (e.g. antivirus purchasing or license renewal, firewall purchase or firewall license renewals, etc.) during the last 3 years (%)

0-5% ☐ 6-10% ☐ 11-15%☐ 16-20% ☐ 21-25% ☐ 26-30% ☐

Do not know ☐

3. Network Communication with External Partners and Collaborators

a. Usage of Secure method or other methods for third party accesses

VPN ☐ TeamViewer ☐ AnyDesk ☐ Remote Desktop ☐

Other secure method ☐ Other unsecure method ☐

b. Communication ports opened and monitored during daily operations (constantly or on demand)

Port TCP 22 (SSH) ☐ Port TCP 23 (Telnet) ☐ Port TCP 3389 (RDP) ☐

Port TCP 20 (FTP data) ☐ Port TCP 21 (FTP control) ☐ other ☐

c. Do existing SLAs include terms that ensure cybersecurity policies are applied by the external partner for preventing data breaches when connected remotely to hospital's information systems?

Yes ☐ No ☐

Do not know ☐

4. Cybersecurity Methods & Practices

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.

a. Does your organization have an Official Cybersecurity Plan?
Yes ☐ No ☐
Do not know ☐
If the previous answer is yes, which of the following plans?
Risk Assessment ☐ Incident Respond Plan ☐ Mitigation plan ☐ Report plan ☐

b. Have any cybersecurity tests been performed in your Organisation during the last 2 years?
Yes ☐ No ☐
If the previous answer is yes, which of the following tests?
Scanning ☐ Penetration ☐ Weak password identification ☐ Phishing ☐
Virus/malware checking ☐ Verification of latest updates/outdates ☐ Other ☐

c. Are you familiar with the Directive (EU) 2016/1148 NIS Directive and GDPR regulation?
Yes ☐ No ☐
Partially ☐

d. Is DDOS attack considered a criminal action according to your National legislation?
Yes ☐ No ☐ Do not know ☐

e. Does your working practice have policies and procedures for the assignment of a unique identifier for each authorized user according to its role?
Yes ☐ No ☐
Do not know ☐

f. Does your working practice have back up information systems so that it can access HIS in the event of an emergency or when your practice's primary systems become unavailable i.e. in the event of a disaster?
Yes ☐ No ☐

g. Do SSL certificates exist for web-based Hospital Information Systems?
Yes ☐ No ☐ Partially ☐

h. Which of the following tools do you use daily for Information Security?

Antivirus/malware	☐	Firewall(s)	☐
Data encryption (data in transit)	☐	Data encryption (data at rest)	☐
Patch & vulnerability management	☐	Intrusion detection systems (IDS)	☐
Network monitoring tools	☐	Mobile device management	☐
User access controls	☐	Intrusion prevention system	☐
Access control lists	☐	Single sign on	☐
Web security gateway	☐	Multi-factor authentication	☐
Data loss prevention (DLP application)	☐	Messaging security gateway	☐
Audit logs of each access to pt. health and financial records			☐
My duties do not include cyber-security activities ☐			

5. Cybersecurity Performance Indicators

a. Percentage of Legacy (unsupported) or known vulnerable systems in place (e.g. end of life operating systems in medical devices) in total equipment (%)
0-10% ☐ 11-20% ☐ 21-30%☐ 31-40% ☐ 41-50% ☐ 51-60% ☐
More than 60% ☐ Do not know ☐

b. Number of cyber security Incidents during the last 3 years (e.g. phishing attacks, virus infections, etc.)?
0-5 ☐ 6-10 ☐ 11-15☐ 16-20 ☐ 21-25 ☐ 26-30 ☐ No records kept ☐

c. Number of unauthorized login attempts in HIS, Active Directory, RIS/PACS per month?
0-5 ☐ 6-10 ☐ 11-15☐ 16-20 ☐ 21-25 ☐ 26-30 ☐
No records kept ☐ No records kept but it is monitored regularly ☐

d. Mean Time to Resolve an Incident?
0-6hours ☐ 7-12hours ☐ 13-24hours☐ 25-48hours ☐ 3-7days ☐
more than a week ☐ No records kept ☐

e. Mean Downtime During an Incident?
0-6 hours ☐ 7-12 hours ☐ 13-24 hours☐ 25-48 hours ☐ 3-7 days ☐
No records kept ☐

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 1: ICT Employees Questionnaire

1. **General Characteristics**
   a. Demographics
      i. Age
         - 21-30 ☐ 31-40 ☐ 41-50 ☐ 51-60 ☐ 61+ ☐
      ii. Gender
         - Male ☐ Female ☐
   b. Education
      - Secondary Education ☐ Vocational training Institution ☐
      - Bachelor Degree ☐ MSc ☐ PhD ☐
   c. Position
      - Doctor ☐ Nurse ☐ Auxiliary personnel ☐ Lab. personnel ☐
      - Administrative personnel ☐ Technical personnel ☐ Other☐
2. **Does your hospital have a Cyber-Security Department or external services?**
   - Yes ☐ No ☐ Do not know ☐
3. **Does your work on the hospital involves working on a computer at any time?**

   Yes ☐ No ☐
4. **Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?**
   - Yes ☐ No ☐
5. **Does your work in the hospital involves access to patient data, which is considered confidential and sensitive information?**
   - Yes ☐ No ☐
6. **Do you have cyber-security policies at your hospital?**
   - Yes ☐ No ☐ Do not know ☐
7. **Do you know when your computer is hacked or infected, and whom to contact when it occurs?**
   a. Yes, I know when my computer is hacked or infected and I know whom to contact.
   b. No, I do not know when my computer is hacked or infected and I don't know whom to contact.
   c. Yes, I know when my computer is hacked or infected but I don't know whom to contact.
   d. No, I do not know when my computer and I know whom to contact.
8. **Have you ever found a virus or Trojan on your computer at work?**
   a. Yes, my computer has been infected before
   b. No, my computer has never been infected
   c. I do not know what a virus or Trojan is
9. **Is anti-virus currently installed on your computer?**
   a. Yes
   b. No
   c. Do not Know
10. **How careful are you when you open an attachment in email?**
    a. I always make sure it is from a person I know and I am expecting the email
    b. As long as I know the person or company that sent me the attachment, I open it
    c. There is nothing wrong with opening attachments
11. **Do you know what a social-engineering attack is?**
    a. Yes, I do
    b. No, I do not
12. **Do you know what an email scam is and how to identify one?**
    a. Yes, I know what an email scam is and how to identify one
    b. I know what an email scam is, but I do not know how to identify one
    c. No, I do not know what an email scam is or how to identify one
13. **My computer has no value to hackers, they do not target me.**
    a. True
    b. False
14. **Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?**

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.

a. Yes
b. No
c. Do not know

15. **Have you downloaded and installed software on your computer at work?**
    a. Yes
    b. No
16. **Have you given your password to your colleagues or your manager, when you were asked for it?**
    a. Yes
    b. No
17. **Which of these is closer to your thinking, even if neither is exactly right?**
    a. Following security policies at our hospital prevents me from doing my job
    b. Following security policies at our hospital helps me do my job better
18. **I feel I have been sufficiently trained in security at our hospital.**
    a. Strongly agree
    b. Agree
    c. Neither agree nor disagree
    d. Disagree
    e. Strongly disagree
19. **I am confident that I could recognize a security issue or incident if I saw one.**
    a. Strongly agree
    b. Agree
    c. Neither agree nor disagree
    d. Disagree
    e. Strongly disagree
20. **Do you lock your PC when you leave your office even for a while?**

    Yes ☐ No ☐

Table 2. Non-ICT Employees Questionnaire

Figures 3 and 4 present the two employees' categories targeted in the questionnaires and the procedures followed to distribute the questionnaires and collect the results. After having the questionnaires translated to the Greek, Romanian and Portuguese languages, invitations were sent to the employees of the three SPHINX end-user partners, requesting them to voluntarily participate in the anonymous surveys online. The requests for participation were shared through the organisation's formal procedures (DYPE5 and HESE) or through social networks (e.g. Facebook) for the POLARIS case and Google forms were used to make the questionnaires accessible online. The project embraced about 11.000 healthcare professionals (9000 in Greece, 1700 in Portugal and 218 in Romania) and approximately 69 ICT employees (60 in Greece, 7 in Portugal and 2 in Romania). It is noted that DYPE5 sent the invitations to 13 supervised hospitals and 60 supervised primary care units. The survey was conducted between September and November 2019.

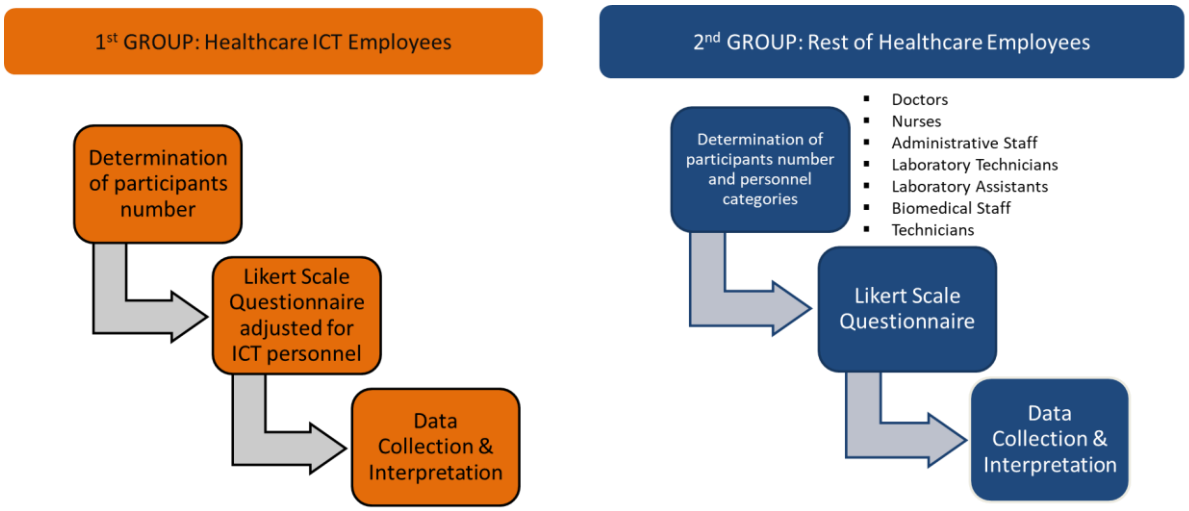

Figure 3: Target Group Determination and Survey Design

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.

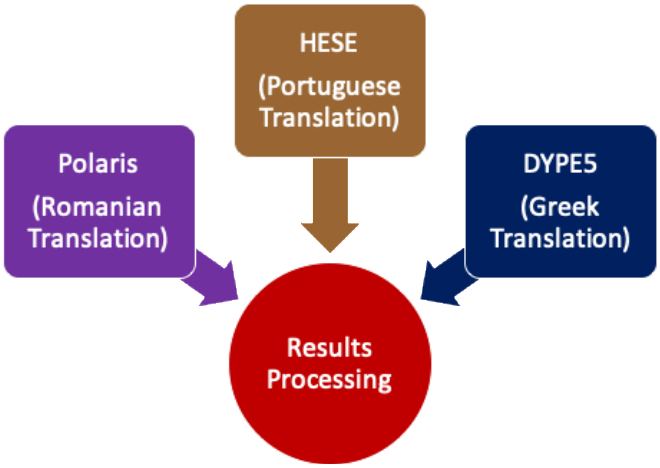

Figure 4: Questionnaires Translation Process and Results Processing

2.2 Questionnaires Results and the Analysis of the Cybersecurity Awareness Status

2.1.1 The ICT Questionnaire

A total of 37 answers were received for the ICT questionnaire, resulting in a 53.6% response rate. The questionnaire's demographic results are shown in Table 3.

	DYPE5	HESE	POLARIS
Number of answers	n = 28 (100%)	n = 7 (100%)	n = 2 (100%)
Gender			
Male	18 (64,3%)	6 (85,7%)	2 (100%)
Female	10 (35,7%)	1 (14,3%)	-
Age			
20-39	9 (32,1%)	2 (28,6%)	-
40-60	19 (67,9%)	5 (71,4%)	2 (100%)
60+	-	-	-
Education			
Secondary Education	4 (14,3%)	3 (42,9%)	-
Vocational training institute	1 (3,6%)	1 (14,3%)	-
Bachelor's degree	16 (57,1%)	1 (14,3%)	1 (50%)
MSc	6 (21,4%)	2 (28,6%)	1 (50%)
PhD	1 (3,6%)	-	-
Years of experience			
0-5	4 (14,3%)	-	-
6-10	3 (10,7%)	1 (14,3%)	-

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.

more than 10	21 (75 %)	6 (85,7%)	2 (100%)
Position			
ICT staff	21 (75%)	6 (85,7%)	1 (50%)
ICT manager	4 (14,3%)	1 (14,3%)	1 (50%)
ICT director	3 (10,7%)	-	-
Healthcare Organisation			
Hospital	25 (89,3%)	7 (100%)	2 (100%)
Clinic	-	-	-
Health Authority	3 (10,7%)	-	-
Organisation Range			
National	-	-	-
Regional	3 (10,7%)	7 (100%)	-
Local	25 (89,3%)	-	2 (100%)
Serving area population			
Population <100k	8 (28,5%)	-	-
Population 100k-300k	15 (53,6%)	1 (14.3%)	-
Population >300k	5 (17,9%)	6 (85.7%)	2 (100%)
Employees in the organisation			
Employees <100	5 (17,9%)	-	-
Employees 100-300	5 (17,9%)	-	2 (100%)
Employees 301-600	1 (3,6%)	-	-
Employees 601-1000	8 (28,5%)	-	-
Employees >1000	9 (32,1%)	7 (100%)	-

Table 3: Demographics of ICT Questionnaire Responses

The evaluation of the ICT questionnaire responses revealed that the proportion of ICT employees in total employment is below 1% for all pilot sites, a percentage that is also below the countries' average as depicted on Figure 2. 46% of the ICT employees reported that, in average, 100K Euros had been spent to procure ICT equipment during the last 2 years (less than 5% from this amount was allocated to cybersecurity appliances, software or hardware). All ICT departments had firewalls and antivirus software installed in their organisations, but official cybersecurity plans were not in place and the incident reporting system is basically absent. Moreover, a separate cybersecurity unit does not exist in the end-users' organisations. The ICT departments do not regularly keep log files of cybersecurity-related events or login actions and cybersecurity-related key performance indicators (KPIs) are not measured. Indeed, almost 50% of ICT employees (aggregated responses) replied that no records are kept for cybersecurity attacks (Figure 5).

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.

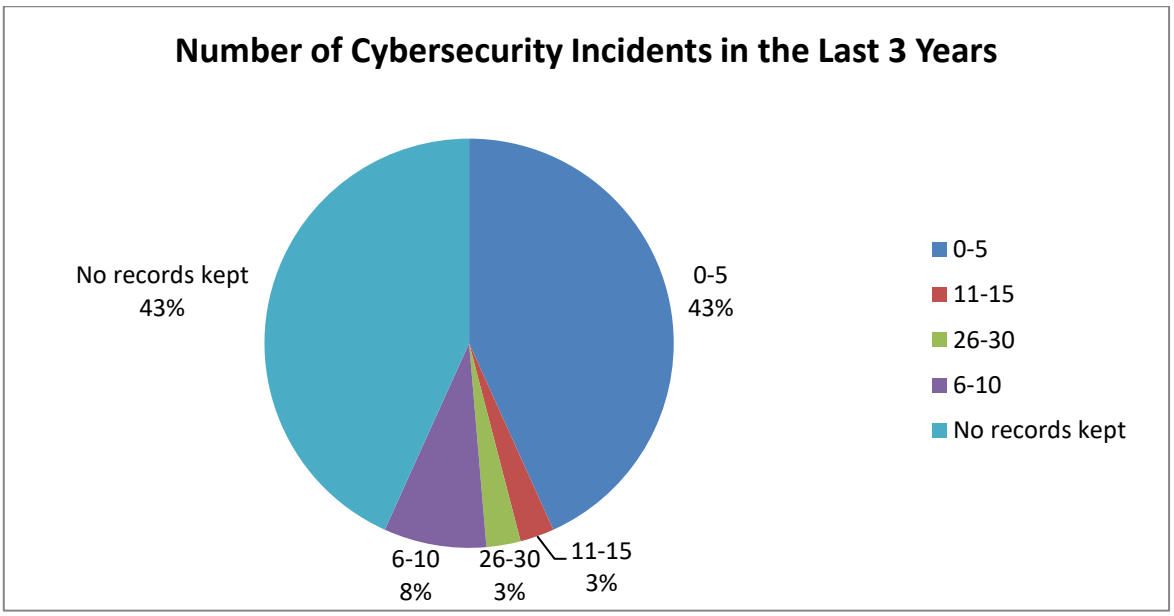

Figure 5: Cybersecurity Incidents in the Last 3 Years

The absence of incident logging reported by almost 50% of the ICT employees is shown in Figure 6:

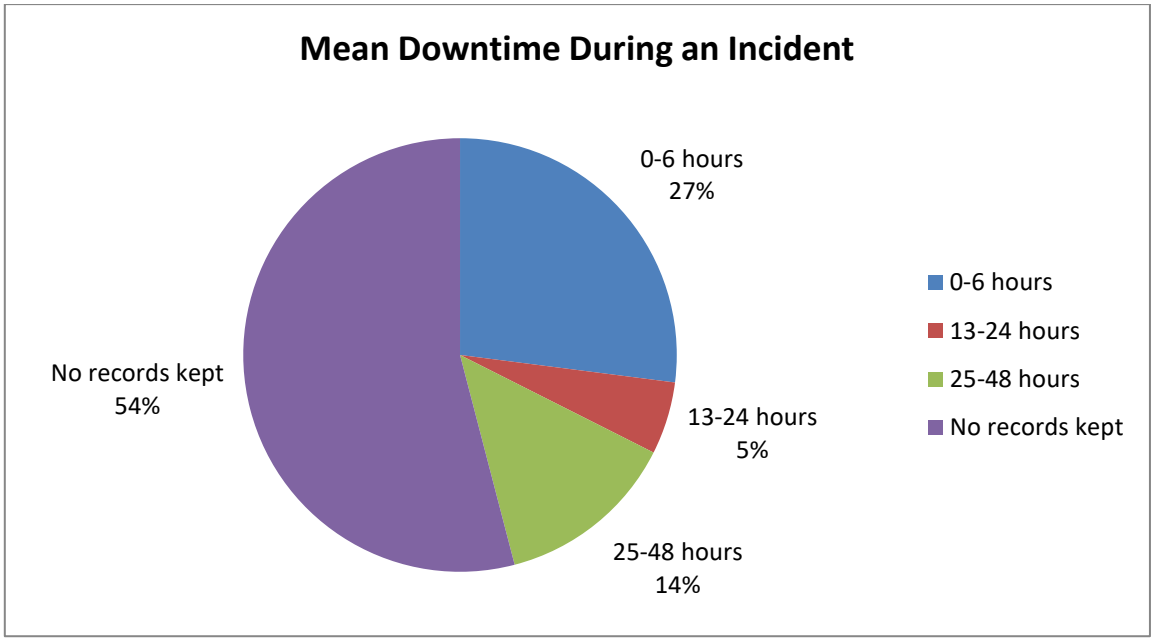

Figure 6: Mean Downtime During an Incident

An additional relevant fact from a cybersecurity perspective relates to the daily use of legacy and vulnerable devices by the healthcare organisation, namely workstations or machines with Windows XP or Windows Embedded operating systems. Although such equipment adds to the vulnerability of the healthcare organisations' ICT infrastructures, these legacy systems cannot be decommissioned since most of them are medical 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.

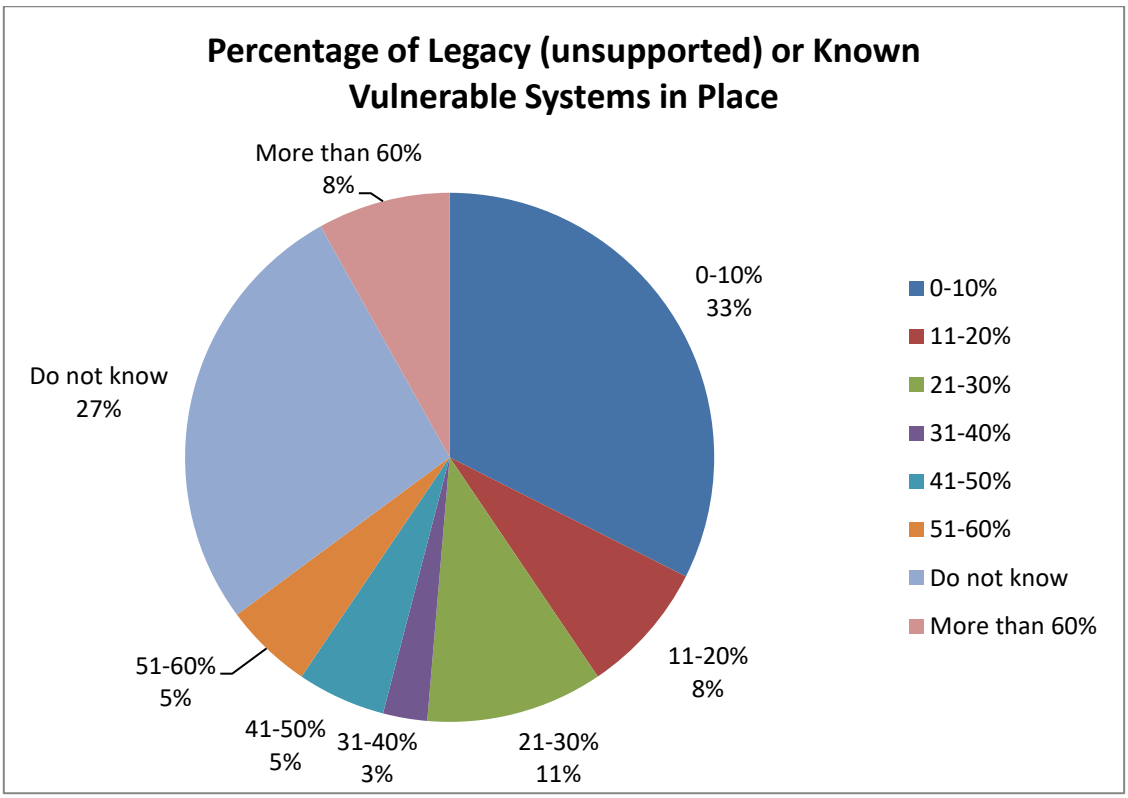

Figure 7: Legacy, Unsupported and Known Vulnerable Systems in Place

Notwithstanding, the questionnaire also revealed that there is a moderate level of cybersecurity awareness and knowledge among ICT employees, mostly because ICT departments are under-staffed, do not execute the required training, do not perform penetration tests and do not have an official cybersecurity policy. It is also noted that the ICT Departments' work is hampered by the absence of methods, tools and cybersecurity procedures. As a result, training to raise the level of cybersecurity awareness is deemed highly important.

Another significant finding is that ICT employees are not aware of the national legislation in force. For example, half of the respondents answered that they do not know whether Distributed Denial of Service (DDOS) attacks are considered criminal actions (Figure 8).

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.

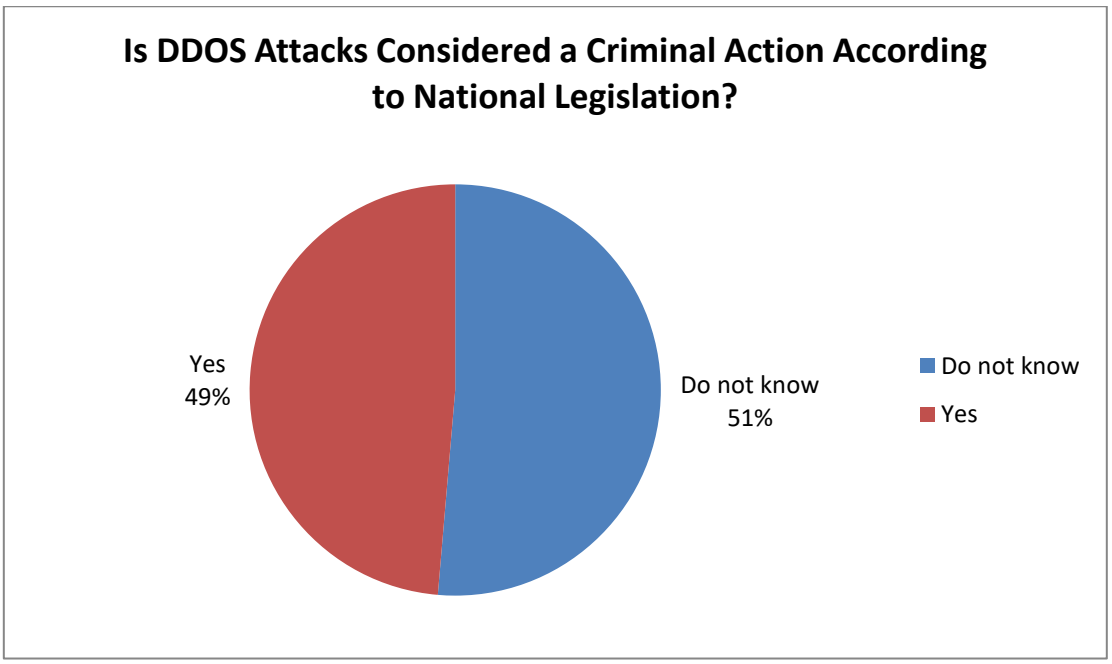

Figure 8: Criminality of Cyber Attacks

Importantly, the questionnaire's responses imply that cybersecurity tests should be organised, for example, by the national Computer Security Incident Response Teams (CSIRTs), in order to assess the current cybersecurity and protection levels against cyber threats and attacks of healthcare organisations.

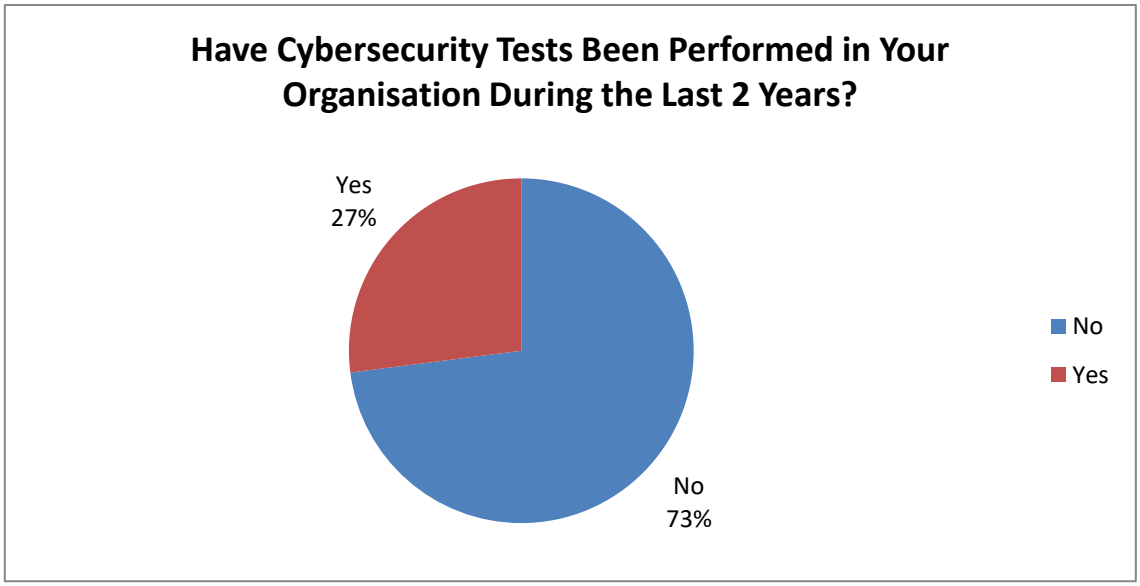

Figure 9: Frequency of Cybersecurity Tests

Annex I provides the detailed analysis of the responses to the ICT questionnaire.

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.

2.1.2 The Non-ICT Questionnaire

A total of 699 answers were received for the non-ICT questionnaire, resulting in a 6.71% response rate. The limited number of responses considering the non-ICT professionals' universe is explained by the reduced time healthcare professionals have to allocate to voluntary external assignments (non-official duty). The questionnaire's demographic results are shown in Table 4.

	DYPE5	HESE	POLARIS
Number of answers	n = 449 (100%)	n = 124 (100 %)	n = 126 (100%)
Gender			
Male	112 (25%)	46 (37,09 %)	21 (16,67%)
Female	337 (75%)	78 (62,91 %)	105 (83,33%)
Age			
21-30	33 (7,3%)	10 (8,06 %)	19 (15,08%)
31-40	91 (20,3%)	36 (29,04 %)	28 (22,22%)
41-50	171 (38,1%)	45 (36,30 %)	66 (52,38%)
51-60	134 (29,8%)	20 (16,12 %)	10 (7,93%)
>61	20 (4,5%)	13 (10,48 %)	3 (2,38%)
Education			
Secondary Education	63 (14,0%)	42 (33,87 %)	9 (7,14%)
Vocational training institute	32 (7,1%)	10 (8,06 %)	10 (7,93%)
Bachelor's degree	247 (55,0%)	5 (4,03 %)	68 (53,97%)
MSc	94 (20,9%)	66 (53,23 %)	29 (23,01%)
PhD	13 (3,0%)	1 (0,81 %)	10 (7,93%)
Position			
Doctor	88 (19,6%)	88 (19,6%)	37 (29,35%)
Nurse	156 (34,7%)	156 (34,7%)	57 (45,23%)
Auxiliary personnel	5 (1,1%)	5 (1,1%)	1 (0,79%)
Lab. personnel	33 (7,4%)	33 (7,4%)	3 (2,38%)
Administrative personnel	127 (28,3%)	127 (28,3%)	23 (18,26%)
Technical personnel	9 (2,0%)	9 (2,0%)	2 (1,59%)
Other	31 (6,9%)	31 (6,9%)	3 (2,38%)

Table 4: Demographics of Non-ICT Questionnaire Responses

The majority of healthcare employees (Doctors, Nurses, Auxiliary, Laboratory, administrative personnel, and technical personnel) answered that the organisation does not have a cybersecurity department, which is in line with the answers of the ICT professionals. Another factor affecting the organisations' cybersecurity protection is the fact that more than 50% of the respondents were not aware of information security policies, albeit they could understand when a computer was hacked or infected and knew whom to contact. This revealed that respondents were not confident about their cybersecurity awareness level.

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.

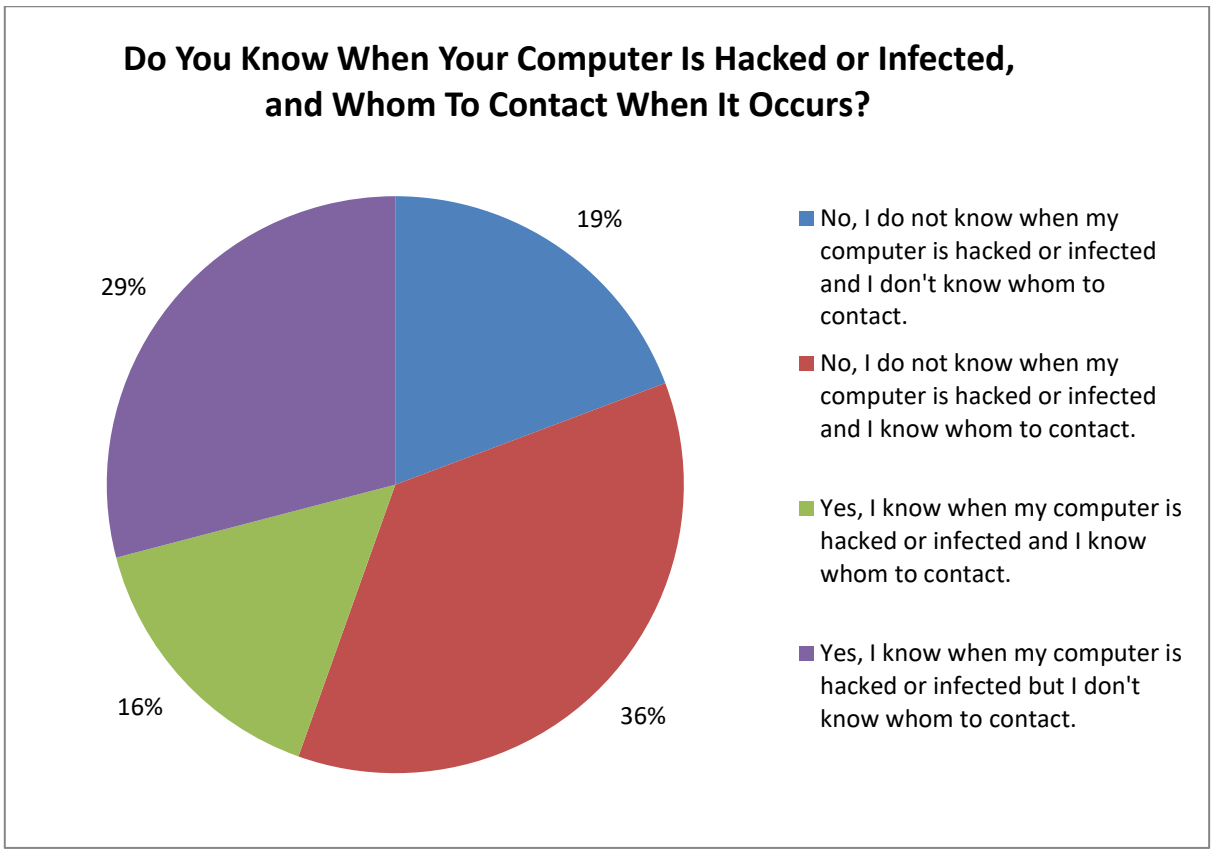

Figure 10: Recognition of Hacked or Infected Computers

More than 50% of the non-ICT professionals answered that their computers had not been infected, while 60% verified whether an anti-virus was installed on their computer and knew how to recognise the presence of such an installation. Approximately 60% of them responded that they trusted the person or company that sent an email with an attachment, so they usually proceeded with opening it. Strangely, they also reported that more than 50% of them did not know what an email fraud was or how to identify it. Furthermore, 75% did not know what a social engineering attack is, nor could they recognise a cybersecurity event. The following figure depicts the behaviour of non-ICT personnel when operating email communications and a direct conclusion is that the majority of email users check the identity of the senders of the electronic messages.

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.

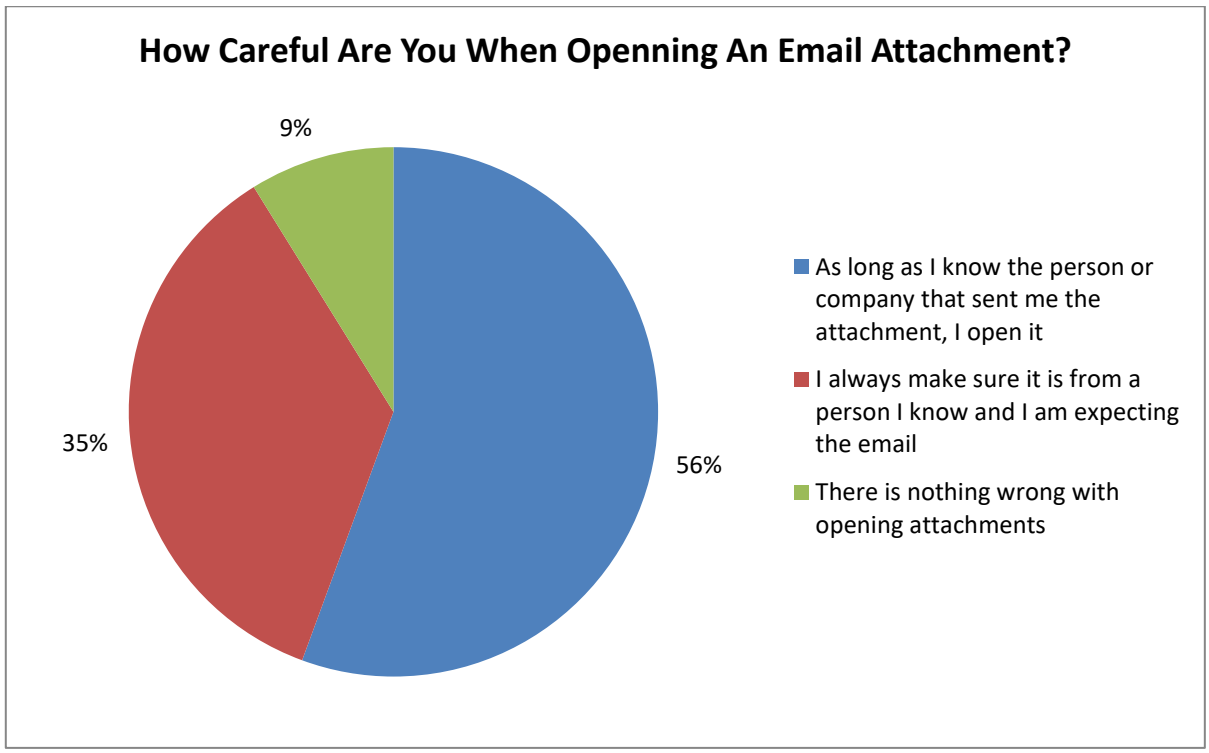

Figure 11: Behaviour Concerning Email Communication

About a fifth of non-ICT employees recognised that they use their own personal devices to store or transfer confidential hospital information, with 16% of non-ICT employees having downloaded and installed software on their computer at work and 30% of them having given their password to colleagues. Notably, half of them do not usually lock their computers when leaving the office.

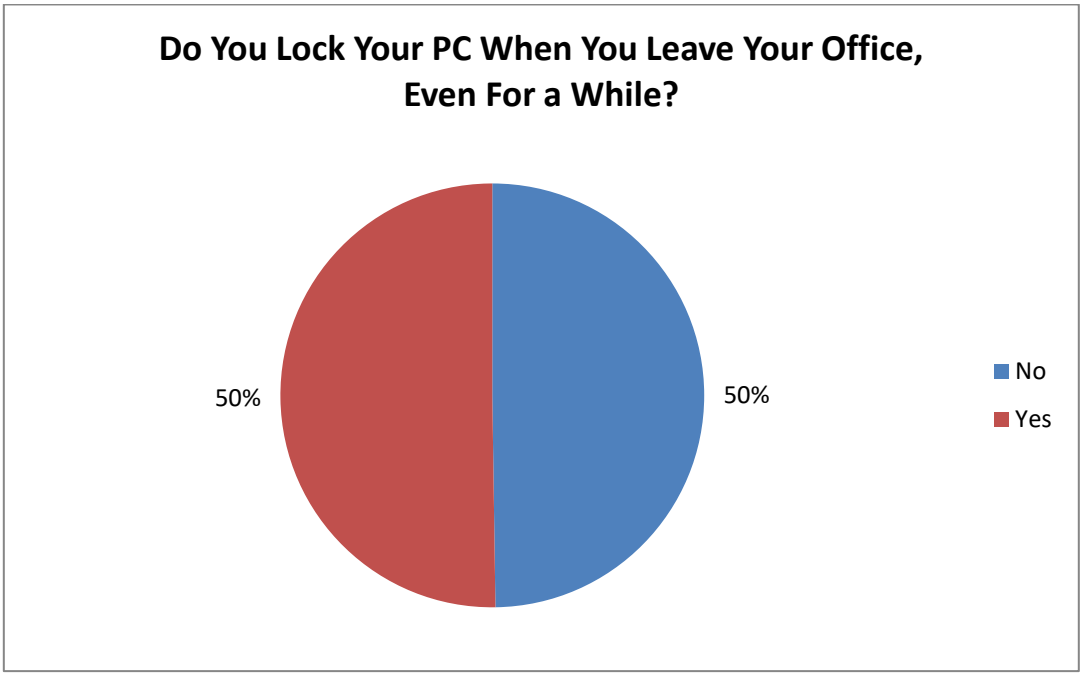

Figure 12: Computer Locking Habits

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 questionnaire responses also revealed that more than 60% of non-ICT professionals have not been officially informed or trained on the GDPR to minimise personal data breaches or cybersecurity incidents, even though more than 65% of the respondents acknowledged that their duties involve access to patient data (75% of them were aware that there is valuable information on the computers they work on), which is considered confidential and sensitive information.

Overall, the non-ICT healthcare professionals considered positive the impact of adopting security policies in their daily activities:

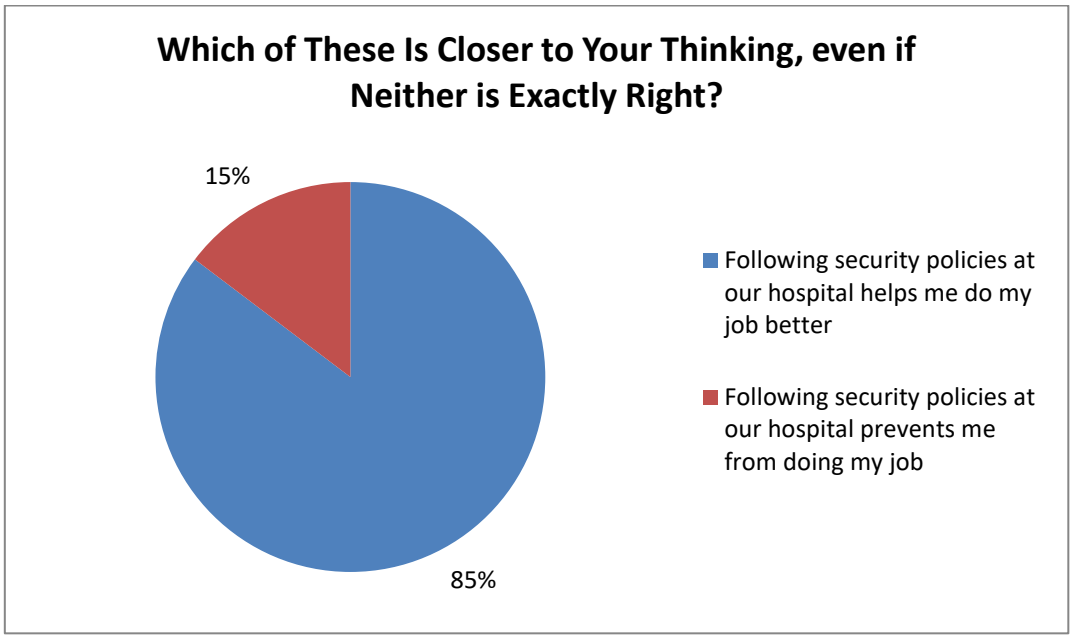

Figure 13: Impact of Security Policies in Daily Work Activities

Table 5 summarises the findings regarding the cyber behaviour and security comprehension level of non-ICT healthcare employees. Indicatively, 25% disagreed that there was a sufficient level of cybersecurity training in the organisation, whereas 27% did not answer; similarly, 23% stated that they could not recognise a cybersecurity problem or incident if one should happen, though 42% did not answer.

Question	Doctor	Nurse	Auxiliary personnel	Laboratory personnel	Administrative personnel	Technical personnel	Other
Do you know when your computer is hacked or infected, and whom to contact when it occurs?	40.8%	42.2%	33.3%	30.2%	42.8%	38.9%	40.5%
Have you ever found a virus or Trojan on your computer at work?	20.4%	23.9%	11.1%	16.3%	20.9%	33.3%	9.5%
Is anti-virus currently installed on your computer?	63.3%	59.6%	44.4%	46.5%	70.6%	66.7%	54.8%
How careful are you when you open an attachment in email?	38.1%	35.7%	27.8%	37.2%	39.3%	33.3%	40.5%
Do you know what a social-engineering attack is?	25.2%	25.7%	22.2%	30.2%	31.3%	33.3%	11.9%

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.

Question	Doctor	Nurse	Auxiliary personnel	Laboratory personnel	Administrative personnel	Technical personnel	Other
Do you know what an email scam is and how to identify one?	27.2%	17.0%	22.2%	23.3%	22.9%	44.4%	14.3%
My computer has no value to hackers, they do not target me.	17.0%	23.5%	44.4%	25.6%	23.4%	22.2%	33.3%
Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?	24.5%	17.0%	22.2%	23.3%	21.9%	33.3%	23.8%
Have you downloaded and installed software on your computer at work?	25.2%	10.9%	27.8%	18.6%	18.4%	38.9%	11.9%
Have you given your password to your colleagues or your manager, when you were asked for it?	21.8%	27.0%	38.9%	14.0%	42.3%	16.7%	50.0%
I feel I have been sufficiently trained in security at our hospital.	19.7%	25.2%	11.1%	25.6%	23.9%	16.7%	19.0%
I am confident that I could recognize a security issue or incident if I saw one.	38.1%	39,6%	16,7%	34,9%	41,3%	33,3%	35,7%
Do you lock your PC when you leave your office even for a while?	55,8%	50,9%	44,4%	46,5%	53,7%	72,2%	52,4%

Table 5: Digital Behaviour and Security Comprehension Level of Healthcare Employees (Answers with YES)

The responses obtained on the recognition of security issues or incidents allow to determine that the behaviour and level of cybersecurity awareness of non-ICT healthcare professionals represent a significant risk factor to the healthcare organisations' cybersecurity. Importantly, 75% of respondents consider that organisational security policies would help improve their own work. Consequently, it is the conclusion of the SPHINX partners that cybersecurity policies should be enforced in the healthcare organisations involved in the SPHINX pilots, assisted with regular cybersecurity awareness training campaigns to disseminate information on the GDPR. The cybersecurity awareness training activities are deemed an effective tool to propagate the adequate cybersecurity policies and measures throughout the organisations. Further, it is the SPHINX Consortium's expectation that the analysis here presented may potentially assist the formulation of specific guidelines and actions to be adopted by and applied in those organisations, in order to cope with cybersecurity issues.

Annex II provides the detailed analysis of the responses to the non-ICT questionnaire.

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 ICT Infrastructure and Assets at the Pilot Sites

This section describes the ICT infrastructure and associated critical assets of the four SPHINX pilot sites in Greece, Romania and Portugal, taking into consideration the European Union Agency for Cybersecurity (ENISA) document *Cyber security and resilience for smart hospitals* [5].

3.1 5th Health Regional Authority of Thessaly and Sterea - Greece

The Information System of the 5th Health Regional Authority (DYPE5) operates on "SYZEFXIS" network, the Greek National State Administration Network (see Figure 14). The SYZEFXIS network is the Internet Service Provider for the Greek State Organisations.

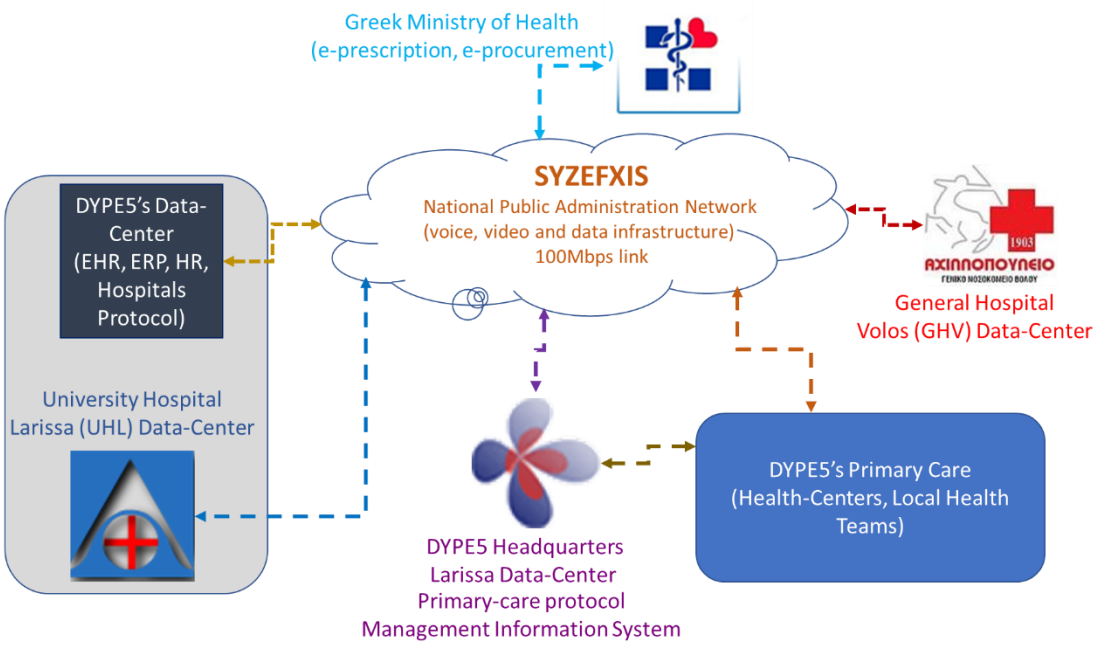

Figure 14: Information System Topology of DYPE5 ICT Infrastructure

The Information Systems of DYPE5, the Hospitals and the Health Centres (Primary Care Organisations) are deployed on two main Data Centres, one installed at the Central Authority's premises and the other at the University Hospital's facilities. The following diagram shows the network topology of these Information 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.

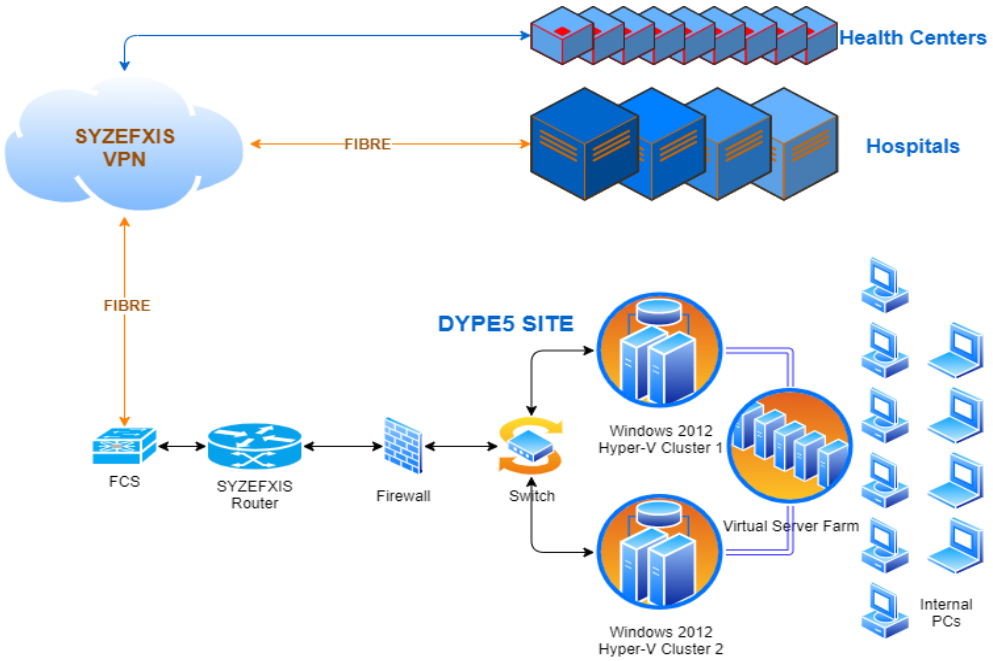

Figure 15: Network Topology of DYPE5 ICT Infrastructure

The two datacentres at DYPE5 have the following hardware characteristics:

- Data Centre 1: 3 Node VMWare Cluster (IBM Servers):
  - each node: 2 x Xeon Processor E5-2640v3, 2.6GHz, 128GB RAM;
  - Storage: 14 x 1.2TB SAS 10K 6Gbps.
- Data Centre 2: 2 Node Hyper-V Cluster (Dell Servers):
  - each node: 2 x Xeon Processor E5-2620v4, 2.1GHz, 128GB RAM;
  - Storage: 24 x 1.2TB SAS 10K 12Gbps.

A brief description of the System and Application servers installed in the two datacentres is given in the following table:

Data Centre 1 (UHL Premises)	Data Centre 2 (Central Authority Premises)
ORACLE APPS 11G	Application Server, IIS, SharePoint Server
NGINX PANEPISTIMIAKO & 5H YPE	Application Server, IIS, SharePoint Server
NGINX VOLOS KOUTLIMPANEIO	Antivirus Server
ORACLE APPS 10G	Database Server
XAAMP (PHP 5.4.31)	Database Server
WAMP (PHP 5.5.12)	Domain Controller
NGINX	Document Management Server
NGINX	Fileserver
ORACLE APPS 12C	Fileserver, IIS, WSUS
ORACLE APPS 12C	Application Server, Database Server, IIS, CMS
LOAD BALANCER NGINX	
DATABASE	
INFRASTRUCTRURE DATABASE	

Table 6: System and Application Servers of DYPE5 Datacentres

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 Information System in the Central Authority presents the following critical assets:

- **Identification systems** - CCTV (video surveillance). These are closed-circuit systems that provide monitoring of indoor / outdoor areas for security reasons.
- **Networking equipment** - Backbone network devices (routers, switches) to support traffic and connectivity.
- **Mobile client devices** - Laptop computers and smartphones.
- **Interconnected clinical information systems** - All clinical information systems of both the University Hospital of Larissa and the General Hospital of Volos operate in Regional Health Authority's 1st datacentre that is located at the UHL's premises. Both hospitals access their information systems following a web architecture. These clinical systems include:
  - Hospital information systems (HIS);
  - Laboratory information systems (LIS);
  - Pharmacy information system (PIS).
- **Proprietary and Health Data -** All financial and administrative data that supports business workflows and procedures (in the 1st and the 2nd Datacentres), including:
  - Accounting system;
  - Billing system;
  - Asset management system;
  - Supply chain;
  - Human Resources system;
  - Payroll;
  - Procurement system;
  - Portal and Website;
  - Electronic protocol and document management system.
- **Buildings and facilities -** The Central Authority is located within the University Hospital Campus. The Central Authority's building is monitored by the UHL's Building Management System (BMS):
  - Power and climate regulation systems, including smart ventilation systems.

3.1.1 University Hospital of Larissa

The Information System at the University Hospital of Larissa presents the following critical assets:

- **Remote care system assets** - The following medical equipment and software is used only for research purposes:
  - Medical equipment for tele-monitoring and tele-diagnosis (e.g. measurements of blood pressure, heart rate, glucose measurements, electrocardiogram or ECG and other remote physiological measurements, threshold-triggered alarm generators). This equipment is in the form of wearables or implantable devices.
  - Telehealth equipment, such as cameras, sensors and telephone/internet connections (e.g. remote radiology diagnosis). There is also a telehealth computer system for patients to register their own physiological measurements (including patient-side application/software, if applicable).
- **Networked medical devices -** The following medical devices are networked:
  - Ultrasounds;
  - Computed tomography (CT);
  - Magnetic resonance imaging (MRI);
  - Angiography;
  - Mammography;

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.

- Coronarography;
- Lithotripter;
- X-Rays;
- X-Ray Digitisers;
- Diagnostic workstations;
- Fluoroscopic C-Arm;
- Thrust Densitometry;
- Radiation Therapy Simulators;
- C-Camera;
- Linear Accelerator.

- **Identification systems -** Identification systems are deployed for security and patient monitoring purposes:
  - Identification systems items such as tags, labels and smart badges (e.g., ultrasound-enabled badges) are used for authentication and, subsequently, authorisation (e.g., allowing access to specific areas);
  - Radio-frequency identification (RFID) systems with location services are used to assess and monitor the movement of assets/patients. These systems are used for beds and live critical patient data monitoring during the entrance and exit of surgery rooms;
  - Closed-circuit television (CCTV) or video surveillance with recognition/authentication capabilities. These are closed-circuit security systems in order to provide authentication, authorisation and monitoring of specific areas.
- **Networking equipment -** The following network and transmission equipment is used for the exchange of data and information:
  - Backbone network devices (e.g., switches, routers). There are Virtual Local Area Network (VLAN) and Quality of Service (QoS) characteristics deployed in order to support big data and high availability;
  - Internet of Things (IoT) Gateways are used (e.g. Cisco, Fortigate) to further analyse data collected by devices and send them to a data centre or the cloud;
  - Specific transmission media is used for academic purposes. There are cameras in the surgery rooms to transmit the surgical operations either via Internet or live aerial connections to remote places in the city of Larissa.
- **Mobile client devices** - the mobile client devices comprise:
  - Mobile clients (e.g., laptop computers, tablets, smartphones, pagers);
  - Mobile applications for smartphone and tablets;
  - Alarm and emergency communication applications for mobile devices.
- **Interconnected clinical information systems** - the following clinical information systems are interconnected:
  - HIS;
  - LIS;
  - PIS;
  - Pathology information system;
  - Blood bank system;
  - Research information system.
- **Proprietary and Health Data -** All financial and administrative data that supports business workflows and procedures, including:
  - Clinical and administrative patient data (e.g. health records, tests results, contact details);
  - Financial, organisational and other hospital 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.

- Research data (e.g. clinical trial reports) and data intended for secondary use;
- Staff data;
- Tracking logs;
- Vendor details (e.g. contact details, products used).

- **Buildings and facilities -** UHL's buildings and facilities are regulated by:
  - Power and climate regulation systems, including smart ventilation systems and a BMS;
  - Temperature sensors;
  - Medical gas supply;
  - Smart patient room operation and management systems, including smart boards, patient screens, medical staff screens;
  - Automated door lock system, including smart locks (e.g., interconnected locks, wireless locks) and lock management.

3.1.2 General Hospital of Volos

The Information System at the General Hospital of Volos presents the following critical assets:

- **Networked medical devices -** The following medical devices are networked:
  - MRI scanner;
  - CT scanner;
  - Ultrasound machines;
  - X-Rays;
  - X- Ray Digitisers;
  - Diagnostic workstations;
  - Cameras and remote assistance for digital surgery rooms;
  - Remote assistance system for cardiac pacemaker implantation room.
- **Networking equipment -** The following network and transmission equipment are used for data and information exchange:
  - Backbone network devices (e.g., switches, routers, wireless access points). VLANs are created in order to support network segmentation;
  - Unified threat management (UTM) firewalls (e.g., Fortigate) are used to secure Internet access.
- **Mobile Client devices -** Laptop computers, tablets and smartphones.
- **Interconnected clinical information systems -** The following systems are currently deployed in the hospital:
  - HIS;
  - LIS;
  - Blood bank system.
- **Proprietary and Health Data** - The data stored and used in the hospital include:
  - Clinical and administrative patient data (e.g. health records, tests results, contact details);
  - Financial, organisational and other hospital data;
  - Research data (e.g. clinical trial reports) and data intended for secondary use;
  - Staff data;
  - Tracking logs;
  - Vendor details (e.g. contact details, products used).
- **Buildings and facilities -** The following systems are used:
  - BMS;
  - Monitoring of temperature sensors;

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.

- CCTV system.

3.2 Polaris Medical - Romania

The Information Systems of Polaris Medical Hospital are depicted in the following diagram (Figure 17). Its Information Systems intercommunicate through an Internet Service provider.

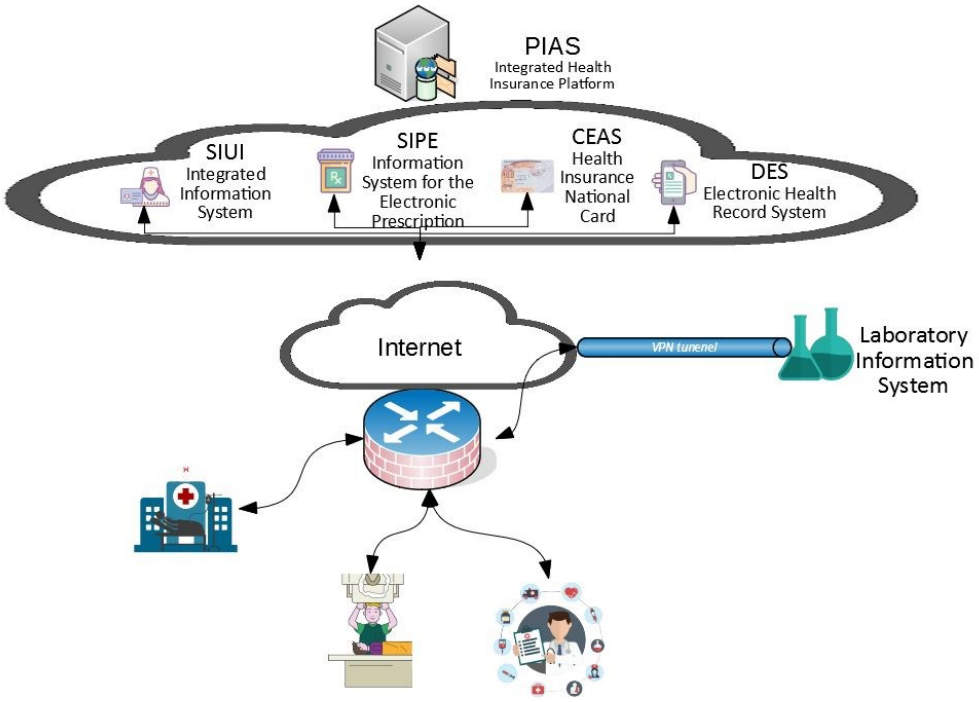

Figure 16: Topology of Information Systems at the Polaris Medical Hospital

The Information Systems at the Polaris Medical Hospital present the following critical assets:

- **Networked medical devices -** A large number of medical devices is utilised such as: Siemens CT system, SAMSUNG RX and ultrasounds machines, EcoNet monitoring equipment, as network medical devices. All images are stored in a Picture Archiving and Communication System (PACS) server and are available to doctors. The images from monitoring devices are stored on a Network Attached Storage (NAS) machine.
- **Identification systems -** In POLARIS, a CCTV network provides monitoring of indoor/outdoor areas for patient's security purposes. Also, an RFID access cards system is used for access in different areas of the hospital. There are different groups of users with access in precise areas. For example, the doctors and nurses have access to patients' rooms, whereas the access in pharmacy's area is closed only to pharmacy's personnel.
- **Networking equipment -** The following network and communication devices are used for data and information exchange:
  - Backbone network devices (e.g. switches, routers, wireless access points). VLANs are created in order to support network segmentation;
  - CISCO Firewalls are used in order to secure internet 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.

- **Mobile Client devices -** Laptop computers, tablets, smartphones and mobile applications for smartphone and tablets;
- **Interconnected clinical information systems -** The following systems are currently working in the hospital environment:
  - SIUI - Integrated Information System;
  - SIPE – Information System for the Electronic Prescription;
  - CEAS - Health Insurance National Card. CEAS objectives are the unique identification of patients who require medical services, recording vital data used for emergency medical situations and reducing fraud against FNUASS.
  - DES - Electronic Health Record System. DES is a centralised database consisting of relevant medical data of patients. Each patient has a unique electronic health record within DES. Healthcare providers can access the historical medical data of a patient. The patient can read his or her medical data through secure access at the EHR system portal. EHR cooperates with other systems that are part of PIAS: SIUI, SIPE and CEAS. The data can be anonymised in order to allow statistical analysis.
  - HIS;
  - PACS for DICOM images provided by RX, CT and ultrasound machines;
  - External Laboratory information system bundled with HIS. It is used a secure Virtual Private Network (VPN) line with a laboratory provider to exchange both requests and results.
- **Proprietary and Health Data -** Data stored and used in the hospital include:
  - Clinical and administrative patient data (e.g. health records, tests results, contact details);
  - Financial, organisational and other hospital data;
  - Personnel data;
  - Tracking logs;
  - Vendor details (e.g. contact details, products used).
- **Buildings and facilities -** For managing the building, the following systems are used:
  - BMS;
  - RFID access control system;
  - CCTV system.

3.3 Hospital do Espírito Santo Évora - Portugal

The HESE information systems are depicted in the following diagram (Figure 17). The HESE network is a subnet of the Internal Health Network managed by the Ministry of Health 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.

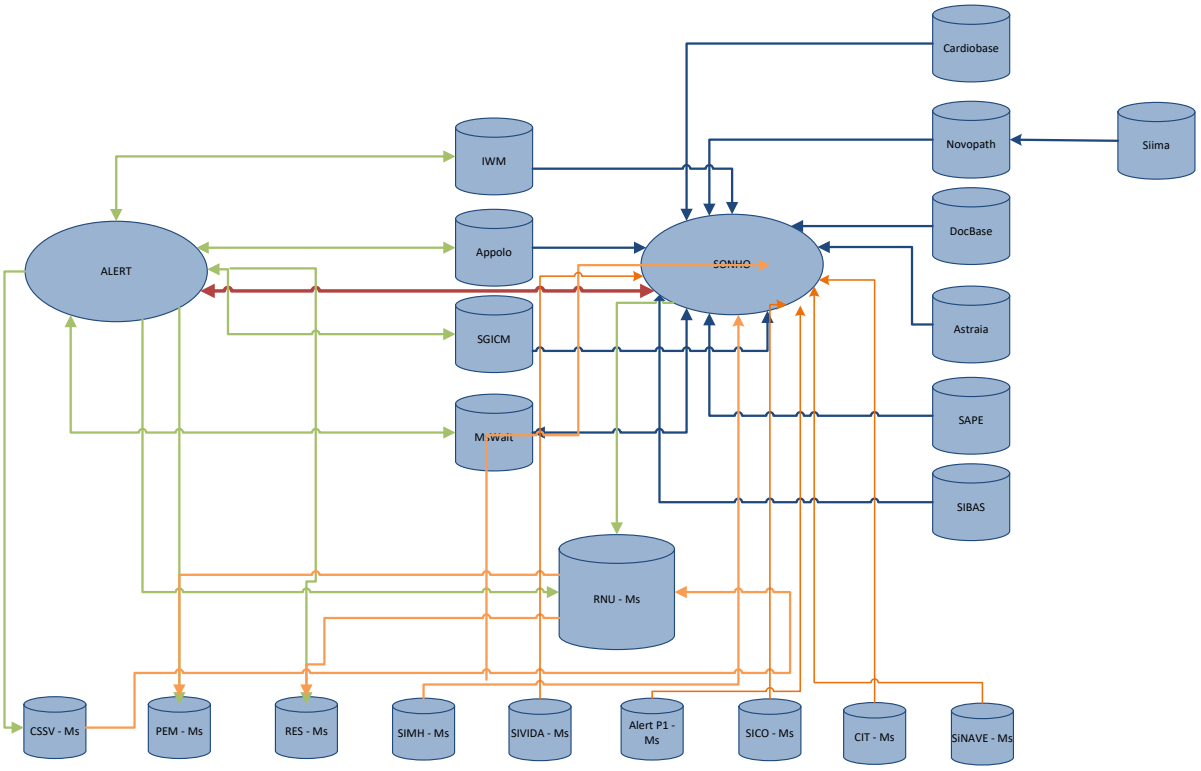

Figure 17: Topology of the Information Systems of the Hospital do Espírito Santo Évora

The Information Systems at HESE present the following critical assets:

- **Remote care system assets -** HESE is one of the hospitals that make the most consultations through telemedicine; the platform is managed by the Ministry of Health and HESE monitors the network traffic from the computer and equipment to its firewall; this system works with a dedicated circuit. In addition, HESE is implementing a new remote patient monitoring system to support the ongoing remote monitoring of patients' health and wellbeing parameters; an App allows patients to register and share the collected data with the doctors through the platform's server in HESE.
- **Networked medical devices -** The ICT infrastructure is separated in two distinct departments: IT and medical equipment. Many medical devices have an associated computer; therefore, the boundary between these departments is unclear. IT is responsible for connecting equipment to the network but the equipment is managed by the medical equipment department or by specialised companies. The IT department monitors the network traffic of all medical equipment connected to the institution's network. The computers associated with the equipment are not connected to the Internet by default and only work on a specific VLAN.
- **Identification systems -** The only identification system in place is for making attendance records by reading the fingerprint.
- **Networking equipment -** The HESE network is a subnet of the Internal Health Network managed by the Ministry of Health Services. About the ministry network, no information about its assets or settings is disclosed. In general, information is sent by two routers in the ministry and received by two other routers/firewalls within the hospital (one in each building). These communications are then forwarded to two routers (one in each building) that communicate over redundant fibres. In addition, there are two lasers that guarantee redundant network operation in case of fibre failure. After firewalls, communications are routed to proxy servers before switching to switches and finally to computers. The same applies in the reverse way. For security reasons, the network is segmented into specific VLANs. There are three types of wireless networks: (1) A network hidden only for assets and without internet

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; (2) A network with internet access for all patients and visitors isolated from the entire infrastructure; and (3) A network provided by the Ministry of Health through a dedicated line, operating in the waiting rooms and having no interaction with the hospital network.

- **Mobile Client devices -** Most mobile devices are used for warehouse and pharmacy inventory control, as well as for blood unit control. In the logistics area, the equipment aims to control advanced warehouses placed in services. When a product is consumed by the patient, the nurse scans the barcode and decreases the number of products in stock. When this number reaches the minimum level, the central warehouse replenishes these products. The software for these devices is prepared with other applications that the hospital has not purchased that allow for safe drug administration per patient. Ensuring medication administration to the patient would be made by comparing the bar code reading of the patient's bracelet and each of the drugs. Other Personal Digital Assistant (PDA) devices work similarly for patient safety when administering blood units. Furthermore, there are also some tablets with specific applications and laptops with network access.
- **Interconnected clinical information systems -** Given the high number of software used by HESE professionals, only the most relevant are mentioned in the relevant diagram. The systems include:
  - SONHO Hospital Information System - This database provides all patients' information to all software working at HESE and receives from it all information recorded for each patient. Recorded information can be used to, for example, charge all treatments done to each patient;
  - ALERT - Electronic health records are made in the ALERT software, from the moment the patient arrives at the hospital until discharge. In the ALERT App, healthcare professionals have access to all patient information, appointments, emergency episodes, operating room and hospitalization. It has interfaces with the LIS, PACS, internal and external medical prescriptions;
  - RIS/PACS - Complete imagiology management service solution that enables viewing, storing, distributing, sharing and printing medical images. It also incorporates functions for complete image manipulation and rendering features;
  - Sibas - Blood bank software;
  - Appolo - Clinical pathology software;
  - Sape - Nursing Records Software;
  - Astraia - Gynaecology and obstetrics software;
  - Docbase - Gastroenterology software;
  - Novopath - Pathologic anatomy software;
  - Cardiobase - Hemodynamics and cardiology software;
  - SGICM - internal Medical Prescription, Dietetics prescription and logistics management software.

  HESE is also connected to central databases provided to the Ministry of Health for all public hospitals and health centres. Some examples are:
  - RNU - Central database with all updated records of each patient;
  - RHnet - Central database with up-to-date records of all healthcare staff;
  - SICO - Central database for death registration;
  - PEM - Central Database of Electronic Medical Prescription;
  - RSE - Application for patients to consult their health data and interact online with family doctors;
  - PDS - The health data platform contains patient information that is shared between hospitals or health centres. This consultation can only be done with the patient's permission. When an access is made, the patient is notified by email or short messages (SMS).
- **Proprietary and Health Data -** except for national databases, all patient data is stored in internal databases and used only at the hospital.
- **Buildings and facilities -** The following systems are used:
  - Monitoring of temperature sensors;

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.

- CCTV system;
- Data Centre alarm system;
- Baby monitoring system (doors are locked automatically in case of sabotage or kidnapping);
- Smoke sensor monitoring;
- Access control 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.

4 SPHINX Pilots Execution Procedures and Evaluation Framework

This section builds on the SPHINX pilots' overview presented in deliverable *D2.4 - Use Cases Definition and Requirements Document v1* to detail the pilot activities to be executed within the SPHINX project, making its association with the SPHINX use cases and identifying the applicable evaluation framework to each of the SPHINX pilots.

4.1 Pilot in Greece: Intra-region Patient Data Transfer

The Pilot involves two of the largest hospitals in DYPE5's jurisdiction, the University Hospital of Larissa (UHL) and the General Hospital of Volos (GHV). GHV (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 40,000sqm). 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, the General Hospital of Volos utilises in its daily operation the Hospital Information System, the Laboratory Information System, the Pharmacy Information System and the Enterprise Resource Planning (ERP) system. Medical workstations coupled to associated Medical Devices are used to expedite patients' treatment plan through digital imaging (DICOM) exchange. A 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.

60km north-west of the city of Volos, in the city of Larissa, UHL 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 specialized 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 System, the Laboratory Information System, the Pharmacy Information System and the Enterprise Resource Planning (ERP) system. Medical workstations coupled to associated Medical Devices are used to expedite patients' treatment plan. A 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.

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.

Both hospitals' HISs are developed and serviced by the same vendor; all the respective application and database servers are hosted in DYPE5's datacenter in Larissa. Access to the health applications, for both hospitals, is web-based and facilitated by the "SYZEFXIS" network, the unified Greek National Public Administration Network, that provides internet and voice services to every Greek Public Body Organisation. Despite the common infrastructure and topology, each hospital's HIS operates as a separate entity, as an obligation by the Greek legal and regulatory framework. Therefore, there is no intra-system and no health data exchange interface between GHV's and UHL's Information Systems.

4.1.1 Pilot Execution Procedures

The Pilot executes the scenario when a patient, originally admitted to the Cardiological Clinic of GHV, gets transferred to UHL's Hemodynamic Lab, to undergo a set of specialised medical tests (e.g. coronary angiography). The doctor in UHL requests access to the patient's Electronic Medical Record that is stored in GHV's Health Information System (Figure 18).

Figure 18: Schematics of the Pilot in Greece: Intra-region Patient Data Transfer Scenario

Despite the legal obligation for the hospitals' information systems to function in separate operations, they are allowed, however, to share personal patient information in a controlled manner. This invokes the intervention of the information system administrator. This workflow sets the scenario for the Pilot and it is described below and depicted in Figure 19:

- The Medical Doctor/Nursing/Administration Staff of UHL contacts (by phone/email) the HIS administration of GHV, asking for medical records of a specific patient that was transferred.
- The Information Technology (IT) department or relevant authorised HIS administration staff of GHV generates a temporary username with a password, to provide access to GHV's HIS.
- Case 1: A web link, within the SYZEFXIS Wide Area Network (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.
- Case 2: 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

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.

via Remote Desktop Protocol (RDP) to a virtual machine or VM (the connection is established through the private WAN of SYZEFXIS) with a LIS client and a 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.

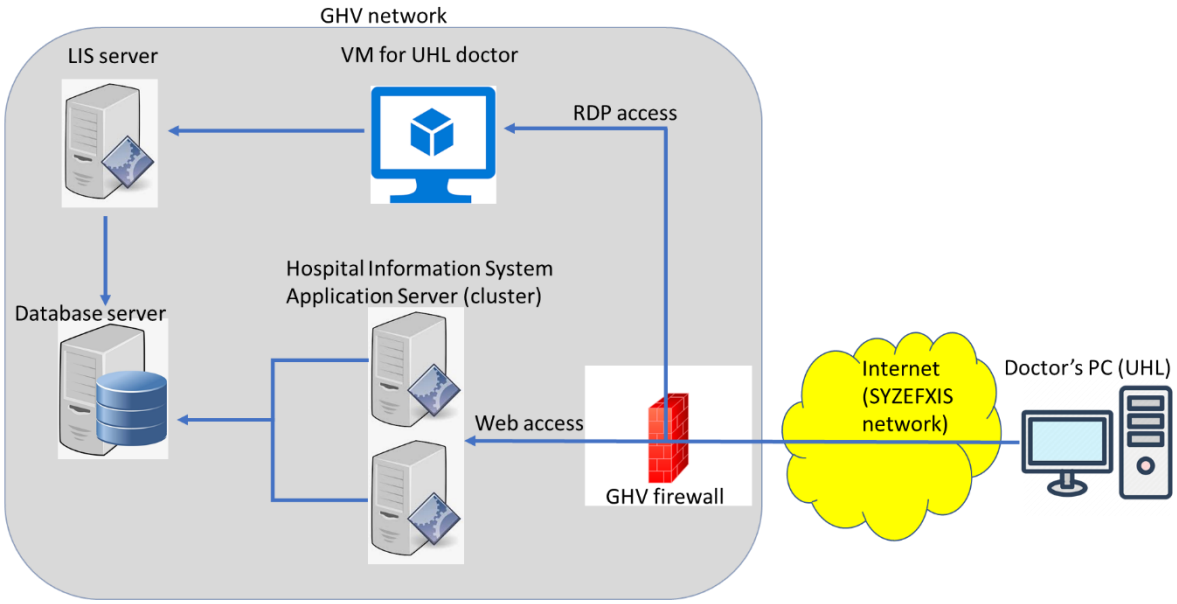

Figure 19: Critical Information Assets Involved in Pilot in Greece: Intra-region Patient Data Transfer

The planning of the Pilot in Greece's test and validation includes the following activities:

- Replication of the HIS and its database in a non-production environment to emulate DYPE5's Hospitals operation during patient admissions;
- Deployment of a safe sandbox environment;
- Simulated patient data (medical diagnosis, medication, test results);
- Utilisation of the SPHINX Toolkit 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).

4.1.2 Applicable SPHINX Use Cases and Tools

A pool of Use Cases has been described in *D2.4 - Use Cases Definition and Requirements Document v1* [1] to drive the SPHINX tools' validation, a set of which correspond to this Pilot's activities:

- UC04: Theft of Health Data by Exploiting Vulnerable Software;
- UC09: Compromised BYOD Enables Stealing of Patient Data;
- UC12: Hacking Health IT Systems (inside attacker).

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 following table establishes the SPHINX tools to be validated in association with the SPHINX Use Cases applicable to the Pilot in Greece. The list of SPHINX tools applicable to the Pilot will be finalised during the execution of Tasks 7.2 and 7.3, upon the contributions from the SPHINX technical partners involved in the SPHINX tools' development, integration and deployment.

Use Case #	Title	Applicable SPHINX Tools to Validate
UC04	**Theft of Health Data by Exploiting Vulnerable Software**	Vulnerability Assessment as a Service (VAaaS), Cyber Security Toolbox (CST), Security Protocol Analysis (SPA), Real-time Cyber Risk Assessment (RCRA), Forensic Data Collection Engine (FDCE), Attack and Behaviour Simulators (ABS), Data Traffic Monitoring (DTM), Anomaly Detection (AD), Interactive Dashboards (ID), Security Information and Event Management (SIEM), Anonymisation and Privacy (AP), Sandbox (SB), Artificial Intelligence Honeypot (HP), Knowledge Base (KB), Machine Learning-empowered Intrusion Detection (MLID), Homomorphic Encryption (HE), Decision Support System (DSS), Analytic Engine (AE), Blockchain Based Threats Registry (BBTR)
UC09	**Compromised BYOD Enables Stealing of Patient Data**	VAaaS, SB, CST, RCRA, DTM, AD, MLID, FDCE, AE, SIEM, SB, DSS, ID, BBTR
UC12	**Hacking Health IT Systems**	VAaaS, CST, SPA, RCRA, FDCE, ABS, DTM, AD, ID, SIEM, AP, SB, HP, KB, MLID, HE, DSS, AE; BBTR

Table 7: Pilot in Greece: Applicable SPHINX Use Cases and Tools

4.1.3 Involved Actors

The Pilot in Greece involves the participation of three actors, representing specific user groups. The list of actors involved in the Pilot and their roles will be finalised during the execution of Tasks 7.2 and 7.3, upon the contributions from the SPHINX technical partners involved in the SPHINX tools' development, integration and deployment.

Actors	Role
IT Operators	Facilitate the remote data access / exchange between hospitals
Medical Professionals	Request and acquire access to a patient's medical records stored in another hospital he was transferred from
Patients and carers	Provide personal health-related information to the Hospital Information System

Table 8: Pilot in Greece: Involved Actors

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.

4.1.4 Evaluation Framework

In SPHINX, abiding to the Specific, Measurable, Attainable, Realistic and Timely (SMART) principle, several KPIs have been defined to adequately assess the effectiveness of the SPHINX Toolkit's critical performance and effectiveness, namely as part of the SPHINX Pilots. In the following table, it is presented the evaluation framework applicable to the Pilot in Greece, enabling to assess if the SPHINX Toolkit meets the objectives proposed for the Pilot.

KPIs for the SPHINX Pilot in Greece		Measure	Assessed Variable	Success Measure
Technical Effectiveness				
KPI 1	Detection of Cybersecurity Events			
KPI 1.1	Number of predicted / forecasted threats	# events/week	Risk, User workload	TBD[1]
KPI 1.2	Number of detected cyber vulnerabilities	# events/week	Risk, User workload	TBD
KPI 1.3	Number of detected unauthorised BYOD accesses	# events/week	Risk, User workload	TBD
KPI 1.4	Number of registered security incidents	# events/week	Risk, User workload	TBD
KPI 1.5	Number of registered abnormal events	# events/week	Risk, User workload	TBD
KPI 1.6	Number of unauthorised accesses to medical devices	# events/week	Risk, User workload	TBD
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 recovery after cyber-attack	hours	Efficiency	< 1
KPI 3	Impact of Cybersecurity Events			
KPI 3.1	Incident impact (per incident)	Ordinal scale (1-5)[2]	Liability risk	TBD
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 update the system	hours	Maintainability	< 1
Automation				
KPI 5	SPHINX Automation			
KPI 5.1	Automation level of security processes	Ordinal scale (1-5)[3]	User workload	4 or higher
User Satisfaction and Usability				
KPI 6	User Satisfaction and Usability			
KPI 6.1	Intuitive presentation	Ordinal scale (1-5)[4]	User acceptance	4 or higher

[1] To be defined.

[2] 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).

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

[4] 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 Pilot in Greece		Measure	Assessed Variable	Success Measure
KPI 6.2	Friendly dashboard	Ordinal scale (1-5)	User acceptance	4 or higher
KPI 6.3	Easy-to-use navigation	Ordinal scale (1-5)	User acceptance	4 or higher
KPI 6.4	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 Toolkit	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.2	Increased trust in eHealth and mHealth services and medical devices	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.3	Adoption of the SPHINX Toolkit	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.4	Increased use of eHealth and mHealth services and medical devices	Ordinal scale (1-5)	Security culture	4 or higher

Table 9: Pilot in Greece: Applicable Evaluation Framework

KPIs for the SPHINX Pilot in Greece		Contributing SPHINX Tools
Technical Effectiveness		
KPI 1	Detection of Cybersecurity Events	
KPI 1.1	Number of predicted / forecasted threats	**RCRA** (risk of cybersecurity incidents); **BBTR** (number of registered threats)
KPI 1.2	Number of detected cyber vulnerabilities	**VAaaS** (number of detected vulnerabilities); **Sandbox** (number of detected vulnerabilities)
KPI 1.3	Number of detected unauthorised BYOD accesses	**SIEM** (number of detected events related with BYOD)
KPI 1.4	Number of registered security incidents	**SIEM** (number of detected events); **AE/DSS** (number of security incidents, using results from HP); **HP** (number of detected entry attempts); **MLID** (number of registered incidents, including previously unknown); **RCRA** (number of triggered alerts)
KPI 1.5	Number of registered abnormal events	**DTM** (number of detected unusual communication (data packets) activity); **AD** (number of detected anomalies); **SIEM** (number of detected events); **AE/DSS** number of security incidents, using results from HP; **HP** (number of detected abnormal activity attempts); **MLID** (number of registered incidents, including previously unknown);
KPI 1.6	Number of unauthorised accesses to medical devices	**SIEM** (number of detected events related with medical 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.

KPIs for the SPHINX Pilot in Greece		Contributing SPHINX Tools
KPI 2	Resolution of Cybersecurity Events	
KPI 2.1	Total time to detect	Based on a user's forensic analysis supported by: - **FDCE** (creation of a timeline of events); - **ID** (display events' timestamp related with various SPHINX services, such as: **SIEM**; **HP**; **DTM**; Assessment of SPHINX performance by simulating attacks using **ABS**.
KPI 2.2	Total time to resolve	Based on a user's forensic analysis supported by: - **FDCE** (creation of a timeline of events); - **ID** (display events' timestamp related with various SPHINX services, such as: **SIEM**; **HP**; **DTM**. Assessment of SPHINX performance by simulating attacks using **ABS**.
KPI 2.3	Service recovery after cyber-attack	User's assessment, assisted by forensic analysis supported by: - **FDCE** (creation of a timeline of events); Assessment of SPHINX performance by simulating attacks using **ABS**.
KPI 3	Impact of Cybersecurity Events	
KPI 3.1	Incident impact (per incident)	User's assessment, supported by: - **FDCE** (creation of a timeline of events); Assessment of SPHINX performance by simulating attacks using **ABS**.
Reliability, Availability and Maintainability		
KPI 4	SPHINX Reliability, Availability and Maintainability	
KPI 4.1	Consistency of results	User's forensics analysis, supported by **FDCE** (creation of a timeline of events). Verifiable when assessing the SPHINX performance from attack simulations using **ABS**.
KPI 4.2	Service availability	**SM** (system operation measurements); **SIEM** (events related with system availability)
KPI 4.3	Total time to update the system	**SM** (system operation measurements); **SIEM** (events related with system updates)
Automation		
KPI 5	SPHINX Automation	
KPI 5.1	Automation level of security processes	Questionnaire
User Satisfaction and Usability		
KPI 6	User Satisfaction and Usability	
KPI 6.1	Intuitive presentation	Questionnaire
KPI 6.2	Friendly dashboard	Questionnaire
KPI 6.3	Easy-to-use navigation	Questionnaire
KPI 6.4	User fatigue	Questionnaire
Cybersecurity Awareness and Behaviour		
KPI 7	Cybersecurity Awareness and Behaviour	
KPI 7.1	Knowledge of cybersecurity best practices	Questionnaire
KPI 7.2	Adoption of cybersecurity behaviours	Questionnaire
KPI 8	Trust and Adoption of SPHINX	
KPI 8.1	Trust in the SPHINX Toolkit	Questionnaire
KPI 8.2	Increased trust in eHealth and mHealth services and medical devices	Questionnaire
KPI 8.3	Adoption of the SPHINX Toolkit	Questionnaire

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 Pilot in Greece		Contributing SPHINX Tools
KPI 8.4	Increased use of eHealth and mHealth services and medical devices	Questionnaire

Table 10: Pilot in Greece: SPHINX Tools Contributing to Applicable Evaluation KPIs

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

4.2.1 Pilot Execution Procedures

The Cross-border Medical Data Exchange Pilot involves the Polaris Medical Clinic (Polaris) from Romania and a DYPE5 hospitals from Greece.

The cross-border scenario is about the case of a Romanian tourist that travels to Greece and needs medical services at the DYPE5 hospital. In order to perform the medical services needed, the doctor from DYPE5 needs to see some of the patient's medical data (CT scans) from Polaris care centre.

To receive the documents needed, the patient sends an e-mail to Polaris, to request access to his medical data. After receiving the patient's e-mail, the Polaris does a brief check-up (patient validation, Polaris doctor agreement) and sends an e-mail with the access link to the web interface of the PACS server. After receiving the e-mail from Polaris, the patient sends it to the DYPE5 doctor. The DYPE5 doctor receives the e-mail and accesses the link to the web interface of the PACS server, to view the requested documents.

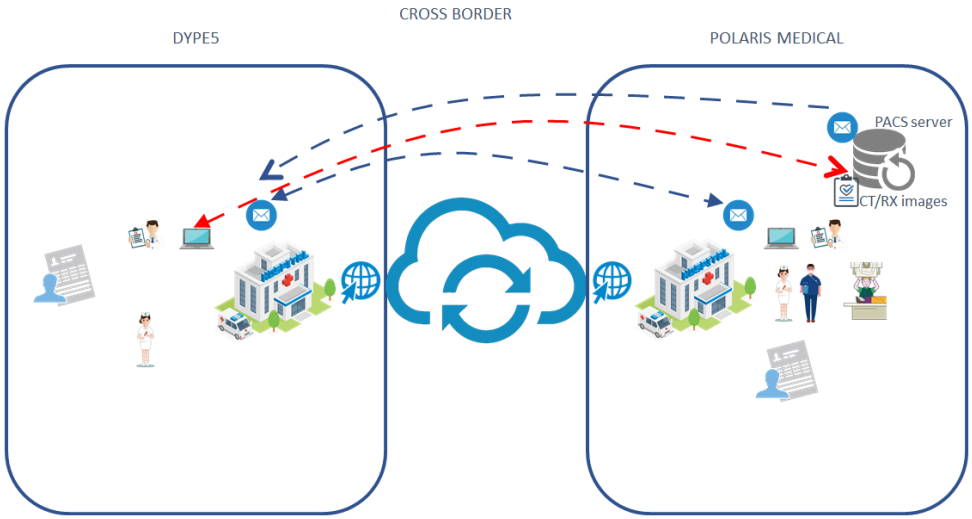

Figure 20: Schematics of the Pilot in Greece and Romania: Cross-Border Medical Data Exchange

The following activities will take place as part of the Cross-border Medical Data Exchange Pilot: a safe sandbox environment will be deployed, replicating the e-mail and PACS server for Polaris and e-mail server and HIS for DYPE5; the patient data will be simulated (DICOM data); the SPHINX toolbox will identify and reduce the cyber vulnerabilities during the data exchange.

The Cross-border Medical Data Exchange Pilot will have the following benefits: improves the trust of the patients and doctors in the cross-border medical data exchange; improves the security levels in the cross border data exchange; improves the overall capabilities of the organisation cyber security; enhances the capability of both Polaris Medical Clinic and DYPE5 hospital to securely interact for patient data exchange; provides time efficient and secure access to patient data in cross-border environments.

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.

4.2.2 Applicable SPHINX Use Cases and Tools

A pool of Use Cases has been described in *D2.4 - Use Cases Definition and Requirements Document v1* [1] to drive the SPHINX tools' validation, a set of which correspond to this Pilot's activities:

- UC06: Ransomware Attack to Healthcare Data;
- UC07: Distributed Denial-of-Service Attack in Regional Hospital;
- UC09: Compromised BYOD Enables Stealing of Patient Data;
- UC12: Hacking Health IT Systems;
- UC16: Intercepting Cross-border Healthcare Data Exchange.

The following table establishes the SPHINX tools to be validated in association with the SPHINX Use Cases applicable to the Pilot in Greece and Romania. The list of SPHINX tools applicable to the Pilot will be finalised during the execution of Tasks 7.2 and 7.3, upon the contributions from the SPHINX technical partners involved in the SPHINX tools' development, integration and deployment.

Use Case #	Title	Applicable SPHINX Tools to Validate
UC06	**Ransomware Attack to Healthcare Data**	VAaaS, RCRA, SPA, DTM, AD, MLID, SB, SIEM, FDCE, DSS, ID, BBTR
UC07	**Distributed Denial-of-Service Attack in Regional Hospital**	VAaaS, SB, DTM, HP, AD, MLID, SIEM, FDCE, DSS, ID, BBTR
UC09	**Compromised BYOD Enables Stealing of Patient Data**	VAaaS, SB, CST, RCRA, DTM, AD, MLID, FDCE, AE, SIEM, SB, DSS, ID, BBTR
UC12	**Hacking Health IT Systems**	VAaaS, CST, SPA, RCRA, FDCE, ABS, DTM, AD, ID, SIEM, AP, SB, HP, KB, MLID, HE, DSS, AE; BBTR
UC16	**Intercepting Cross-border Healthcare Data Exchange**	VAaaS, SB, S-API, SPA, DTM, AD, MLID, SIEM, FDCE, DSS, ID, BBTR

Table 11: Pilot in Greece and Romania: Applicable SPHINX Use Cases and Tools

4.2.3 Involved Actors

The Pilot in Greece and Romania involves the participation of six actors, representing specific user groups. The list of actors involved in the Pilot and their roles will be finalised during the execution of Tasks 7.2 and 7.3, upon the contributions from the SPHINX technical partners involved in the SPHINX tools' development, integration and deployment.

Actors	Role
Romanian Tourist (patient)	Requests access to his medical records in Romania, while in Greece
Doctor in DYPE5 hospital	Receives patient's email with the access to the patient's medical records stored in Romania

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.

Actors	Role
Clerk in POLARIS	Receives the patient's access request to his medical records and validates the identity of the patient; requests the doctor's authorisation and the required imagery from the imagery technician
Imagery technician in POLARIS	Receives a validated request for a patient's imagery and provides the access link to the web interface of the PACS system
Doctor in POLARIS	Authorises the (validated) patient's access to his medical records

Table 12: Pilot in Greece and Romania: Involved Actors

4.2.4 Evaluation Framework

In SPHINX, abiding to the SMART principle, several KPIs have been defined to adequately assess the effectiveness of the SPHINX Toolkit's critical performance and effectiveness, namely as part of the SPHINX Pilots. In the following table, it is presented the evaluation framework applicable to the Pilot in Greece and Romania, enabling to assess if the SPHINX Toolkit meets the objectives proposed for the Pilot.

KPIs for the SPHINX Pilot in Greece and Romania		Measure	Assessed Variable	Success Measure
Technical Effectiveness				
KPI 1	Detection of Cybersecurity Events			
KPI 1.1	Number of predicted / forecasted threats	# events/week	Risk, User workload	TBD
KPI 1.2	Number of detected cyber vulnerabilities	# events/week	Risk, User workload	TBD
KPI 1.3	Number of detected unauthorised BYOD accesses	# events/week	Risk, User workload	TBD
KPI 1.5	Number of registered abnormal events	# events/week	Risk, User workload	TBD
KPI 1.6	Number of unauthorised accesses to medical devices	# events/week	Risk, User workload	TBD
KPI 2	Resolution of Cybersecurity Events			
KPI 2.1	Total time to detect	minutes	Efficiency	< 1
KPI 2.3	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)	Liability risk	TBD
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%
Automation				
KPI 5	SPHINX Automation			
KPI 5.1	Automation level of security processes	Ordinal scale (1-5)	User workload	4 or higher

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 Pilot in Greece and Romania		Measure	Assessed Variable	Success Measure
User Satisfaction and Usability				
KPI 6	User Satisfaction and Usability			
KPI 6.1	Intuitive presentation	Ordinal scale (1-5)	User acceptance	4 or higher
KPI 6.2	Friendly dashboard	Ordinal scale (1-5)	User acceptance	4 or higher
KPI 6.3	Easy-to-use navigation	Ordinal scale (1-5)	User acceptance	4 or higher
KPI 6.4	User fatigue	%	User acceptance	< 5%
Cybersecurity Awareness and Behaviour				
KPI 7	Cybersecurity Awareness and Behaviour			
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 Toolkit	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.2	Increased trust in eHealth and mHealth services and medical devices	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.3	Adoption of the SPHINX Toolkit	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.4	Increased use of eHealth and mHealth services and medical devices	Ordinal scale (1-5)	Security culture	4 or higher

Table 13: Pilot in Greece and Romania: Applicable Evaluation Framework

KPIs for the SPHINX Pilot in Greece and Romania		Contributing SPHINX Tools
Technical Effectiveness		
KPI 1	Detection of Cybersecurity Events	
KPI 1.1	Number of predicted / forecasted threats	**RCRA** (risk of cybersecurity incidents); **BBTR** (number of registered threats)
KPI 1.2	Number of detected cyber vulnerabilities	**VAaaS** (number of detected vulnerabilities); **Sandbox** (number of detected vulnerabilities)
KPI 1.3	Number of detected unauthorised BYOD accesses	**SIEM** (number of detected events related with BYOD)
KPI 1.5	Number of registered abnormal events	**DTM** (number of detected unusual communication (data packets) activity); **AD** (number of detected anomalies); **SIEM** (number of detected events); **AE/DSS** number of security incidents, using results from HP; **HP** (number of detected abnormal activity attempts); **MLID** (number of registered incidents, including previously unknown)
KPI 1.6	Number of unauthorised accesses to medical devices	**SIEM** (number of detected events related with medical devices)
KPI 2	Resolution of Cybersecurity Events	
KPI 2.1	Total time to detect	Based on a user's forensic analysis supported by: - **FDCE** (creation of a timeline of events); - **ID** (display events' timestamp related with various SPHINX services, such as: **SIEM**; **HP**; **DTM**; Assessment of SPHINX performance by simulating attacks using **ABS**.

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 Pilot in Greece and Romania		Contributing SPHINX Tools
KPI 2.3	Service recovery after cyber-attack	User's assessment, assisted by forensic analysis supported by: - **FDCE** (creation of a timeline of events); Assessment of SPHINX performance by simulating attacks using **ABS**.
KPI 3	Impact of Cybersecurity Events	
KPI 3.1	Incident impact (per incident)	User's assessment, supported by: - **FDCE** (creation of a timeline of events); Assessment of SPHINX performance by simulating attacks using **ABS**.
Reliability, Availability and Maintainability		
KPI 4	SPHINX Reliability, Availability and Maintainability	
KPI 4.1	Consistency of results	User's forensics analysis, supported by **FDCE** (creation of a timeline of events). Verifiable when assessing the SPHINX performance from attack simulations using **ABS**.
KPI 4.2	Service availability	**SM** (system operation measurements); **SIEM** (events related with system availability)
Automation		
KPI 5	SPHINX Automation	
KPI 5.1	Automation level of security processes	Questionnaire
User Satisfaction and Usability		
KPI 6	User Satisfaction and Usability	
KPI 6.1	Intuitive presentation	Questionnaire
KPI 6.2	Friendly dashboard	Questionnaire
KPI 6.3	Easy-to-use navigation	Questionnaire
KPI 6.4	User fatigue	Questionnaire
Cybersecurity Awareness and Behaviour		
KPI 7	Cybersecurity Awareness and Behaviour	
KPI 7.2	Adoption of cybersecurity behaviours	Questionnaire
KPI 8	Trust and Adoption of SPHINX	
KPI 8.1	Trust in the SPHINX Toolkit	Questionnaire
KPI 8.2	Increased trust in eHealth and mHealth services and medical devices	Questionnaire
KPI 8.3	Adoption of the SPHINX Toolkit	Questionnaire
KPI 8.4	Increased use of eHealth and mHealth services and medical devices	Questionnaire

Table 14: Pilot in Greece and Romania: SPHINX Tools Contributing to Applicable Evaluation KPIs

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

4.3.1 Pilot Execution Procedures

The Pilot in Portugal, entitled *Securing Advanced Patient Care in Hospital and Homecare Environments* explores the incorporation of modern medical and healthcare connected devices to support patient care,

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.

enabling monitoring on a 24/7 basis of patients placed both in hospital and home environments. This pilot is conducted by Évora's Espírito Santo Hospital (HESE), which provides the hospital's environment and the end-user's perspective, supported by EDGE, which delivers the technological platform supporting remote patient care.

The hospital's environment is a well-controlled and secure environment, adopts best security policies, practices and processes and is managed by well-trained and specialised staff. However, the utilisation of connected medical devices exhibiting cybersecurity vulnerabilities (see *D2.1 - Advanced Cyber Security Threats Digest and Analysis* [6]) brings many challenges to securing the hospital IT ecosystem. In addition, remote patient care at home settings require hospitals to interact with an uncontrolled and untrusted environment managed by non-IT specialists (i.e., the patient), likely involving the use of Bring Your Own Device (BYOD) without application restrictions. The Pilot in Portugal therefore brings forth numerous challenges and threats in what respects the hospital's cybersecurity and assurance of patients' data privacy, protection, confidentiality and trust.

An overview of the Pilot in Portugal is presented Figure 21. The figure depicts, on the one hand, the hospital IT environment and, on the other hand, the remote home environment involving the patient's devices:

- The Healthcare IT Environment comprises:
  - the Hospital's information systems;
  - EDGE's eCare Platform for advanced patient care, which collects health and wellbeing information from health and mobile devices to assist in hospital and remote (at home) care;
  - connected devices that measure health-related parameters from patients and transmit them over the network;
  - SPHINX tools that are a result of the SPHINX Project and provide advanced cybersecurity tools for situational awareness, decision support and device certification. SPHINX tools may also include extensions and add-ons provided by third-parties.
- The Remote Home Environment refers to the patient's space and involves the use of mobile devices (BYOD) and connected equipment to collect and manage health and wellbeing information.

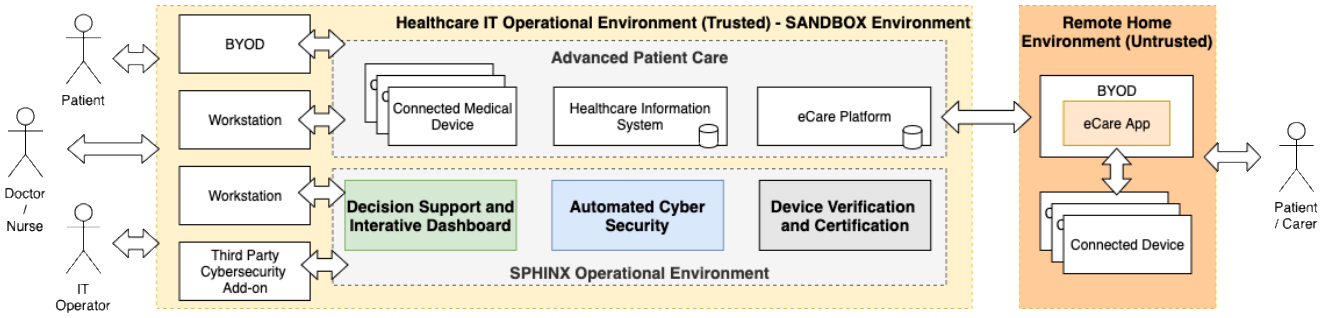

Figure 21: Schematics of the Pilot in Portugal: Securing Advanced Patient Care in Hospital and Homecare Environments

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, 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);

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.

- Utilisation of the SPHINX Toolkit 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).

4.3.2 Applicable SPHINX Use Cases and Tools

A pool of Use Cases has been described in *D2.4 - Use Cases Definition and Requirements Document v1* [1] to drive the SPHINX tools' validation, a set of which correspond to this Pilot's activities:

- Use Case 05: Tampering with Medical Devices;
- Use Case 10: Taking Control of a Connected Medical Device;
- Use Case 12: Hacking Health IT Systems;
- Use Case 13: Exploiting Remote Patient Monitoring Services;
- Use Case 18: Accessing Health Data in Fitness App;
- Use Case 19: Transfer of Medical Devices Between Healthcare Providers.

The following table establishes the SPHINX tools to be validated in association with the SPHINX Use Cases applicable to the Pilot in Portugal. The list of SPHINX tools applicable to the Pilot will be finalised during the execution of Tasks 7.2 and 7.3, upon the contributions from the SPHINX technical partners involved in the SPHINX tools' development, integration and deployment.

Use Case #	Title	Applicable SPHINX Tools to Validate
UC05	**Tampering with Medical Devices**	S-API, SB, VAaaS, RCRA, AD, MLID, SIEM, FDCE, DSS, ID
UC10	**Taking Control of a Connected Medical Device**	VAaaS, SB, AD, MLID, SIEM, FDCE, DSS, ID
UC12	**Hacking Health IT Systems**	VAaaS, CST, SPA, RCRA, FDCE, ABS, DTM, AD, SIEM, AP, SB, HP, KB, MLID, HE, DSS, AE, ID BBTR
UC13	**Exploiting Remote Patient Monitoring Services**	VAaaS, SPA, RCRA, SIEM, FDCE, DSS, ID
UC18	**Accessing Health Data in Fitness App**	S-API, SB, VAaaS, SPA, DTM, AD, SIEM, FDCE, DSS, ID
UC19	**Transfer of Medical Devices Between Healthcare Providers**	S-API, SB, VAaaS, HP, AD, SIEM, FDCE, DSS, ID

Table 15: Pilot in Portugal: Applicable SPHINX Use Cases and Tools

4.3.3 Involved Actors

The Pilot in Portugal involves the participation of three actors, representing specific user groups. The list of actors involved in the Pilot and their roles will be finalised during the execution of Tasks 7.2 and 7.3, upon the contributions from the SPHINX technical partners involved in the SPHINX tools' development, integration and deployment.

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.

Actors	Role
Hospital IT Operators	The professionals responsible for the implementation and monitoring of the hospital's cybersecurity. They are the ones operating the SPHINX Tools, benefitting from their advanced automated functionalities in order to enhance in-place cybersecurity defences and improve the level of cybersecurity awareness at the hospital. IT operators use workstations provided by the hospital
Doctors and Nurses	The medical professionals that use the connected devices and access health and wellbeing information from the eCare Platform and other hospital's information systems. The medical professionals use workstations provided by the hospital and BYOD devices
Patients and Carers	The users who are monitored from their home, and use connected health devices and their BYOD devices to access the eCare Platform via the eCare App to provide or access their own personal health-related information. Alternatively, patients may receive support of carers that access the eCare Platform on behalf of the patients.

Table 16: Pilot in Portugal: Involved Actors

4.3.4 Evaluation Framework

In SPHINX, abiding to the SMART principle, several KPIs have been defined to adequately assess the effectiveness of the SPHINX Toolkit's critical performance and effectiveness, namely as part of the SPHINX Pilots (*D2.4 - Use Cases Definition and Requirements Document v1* [1]). In the following table, it is presented the evaluation framework applicable to the Pilot in Portugal, enabling to assess if the SPHINX Toolkit meets the objectives proposed for the Pilot.

KPIs for the SPHINX Pilot in Portugal		Measure	Assessed Variable	Success Measure
Technical Effectiveness				
KPI 1	Detection of Cybersecurity Events			
KPI 1.1	Number of predicted / forecasted threats	# events/week	Risk, User workload	TBD
KPI 1.2	Number of detected cyber vulnerabilities	# events/week	Risk, User workload	TBD
KPI 1.3	Number of detected unauthorised BYOD accesses	# events/week	Risk, User workload	TBD
KPI 1.4	Number of registered security incidents	# events/week	Risk, User workload	TBD
KPI 1.5	Number of registered abnormal events	# events/week	Risk, User workload	TBD
KPI 1.6	Number of unauthorised accesses to medical devices	# events/week	Risk, User workload	TBD
KPI 2	Resolution of Cybersecurity Events			
KPI 2.1	Total time to detect	minutes	Efficiency	< 1

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 Pilot in Portugal		Measure	Assessed Variable	Success Measure
KPI 2.2	Total time to resolve	hours	Efficiency	< 1
KPI 2.3	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)	Liability risk	TBD
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%
Automation				
KPI 5	SPHINX Automation			
KPI 5.1	Automation level of security processes	Ordinal scale (1-5)	User workload	4 or higher
User Satisfaction and Usability				
KPI 6	User Satisfaction and Usability			
KPI 6.1	Intuitive presentation	Ordinal scale (1-5)	User acceptance	4 or higher
KPI 6.2	Friendly dashboard	Ordinal scale (1-5)	User acceptance	4 or higher
KPI 6.3	Easy-to-use navigation	Ordinal scale (1-5)	User acceptance	4 or higher
Cybersecurity Awareness and Behaviour				
KPI 7	Cybersecurity Awareness and Behaviour			
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 Toolkit	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.2	Increased trust in eHealth and mHealth services and medical devices	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.3	Adoption of the SPHINX Toolkit	Ordinal scale (1-5)	Security culture	4 or higher
KPI 8.4	Increased use of eHealth and mHealth services and medical devices	Ordinal scale (1-5)	Security culture	4 or higher

Table 17: Pilot in Portugal: Applicable Evaluation Framework

KPIs for the SPHINX Pilot in Portugal		Contributing SPHINX Tools
Technical Effectiveness		
KPI 1	Detection of Cybersecurity Events	
KPI 1.1	Number of predicted / forecasted threats	**RCRA** (risk of cybersecurity incidents); **BBTR** (number of registered threats)
KPI 1.2	Number of detected cyber vulnerabilities	**VAaaS** (number of detected vulnerabilities); **Sandbox** (number of detected vulnerabilities)
KPI 1.3	Number of detected unauthorised BYOD accesses	**SIEM** (number of detected events related with BYOD)
KPI 1.4	Number of registered security incidents	**SIEM** (number of detected events); **AE/DSS** (number of security incidents, using results from HP); **HP** (number of detected entry attempts); **MLID** (number of registered incidents, including previously unknown); **RCRA** (number of triggered alerts)

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 Pilot in Portugal		Contributing SPHINX Tools
KPI 1.5	Number of registered abnormal events	**DTM** (number of detected unusual communication (data packets) activity); **AD** (number of detected anomalies); **SIEM** (number of detected events); **AE/DSS** number of security incidents, using results from HP; **HP** (number of detected abnormal activity attempts); **MLID** (number of registered incidents, including previously unknown)
KPI 1.6	Number of unauthorised accesses to medical devices	**SIEM** (number of detected events related with medical devices)
KPI 2	Resolution of Cybersecurity Events	
KPI 2.1	Total time to detect	Based on a user's forensic analysis supported by: - **FDCE** (creation of a timeline of events); - **ID** (display events' timestamp related with various SPHINX services, such as: **SIEM**; **HP**; **DTM**; Assessment of SPHINX performance by simulating attacks using **ABS**.
KPI 2.2	Total time to resolve	Based on a user's forensic analysis supported by: - **FDCE** (creation of a timeline of events); - **ID** (display events' timestamp related with various SPHINX services, such as: **SIEM**; **HP**; **DTM**. Assessment of SPHINX performance by simulating attacks using **ABS**.
KPI 2.3	Service recovery after cyber-attack	User's assessment, assisted by forensic analysis supported by: - **FDCE** (creation of a timeline of events); Assessment of SPHINX performance by simulating attacks using **ABS**.
KPI 3	Impact of Cybersecurity Events	
KPI 3.1	Incident impact (per incident)	User's assessment, supported by: - **FDCE** (creation of a timeline of events); Assessment of SPHINX performance by simulating attacks using **ABS**.
Reliability, Availability and Maintainability		
KPI 4	SPHINX Reliability, Availability and Maintainability	
KPI 4.1	Consistency of results	User's forensics analysis, supported by **FDCE** (creation of a timeline of events). Verifiable when assessing the SPHINX performance from attack simulations using **ABS**.
KPI 4.2	Service availability	**SM** (system operation measurements); **SIEM** (events related with system availability)
Automation		
KPI 5	SPHINX Automation	
KPI 5.1	Automation level of security processes	Questionnaire
User Satisfaction and Usability		
KPI 6	User Satisfaction and Usability	
KPI 6.1	Intuitive presentation	Questionnaire
KPI 6.2	Friendly dashboard	Questionnaire
KPI 6.3	Easy-to-use navigation	Questionnaire
Cybersecurity Awareness and Behaviour		
KPI 7	Cybersecurity Awareness and Behaviour	
KPI 7.2	Adoption of cybersecurity behaviours	Questionnaire
KPI 8	Trust and Adoption of SPHINX	
KPI 8.1	Trust in the SPHINX Toolkit	Questionnaire

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 Pilot in Portugal		Contributing SPHINX Tools
KPI 8.2	Increased trust in eHealth and mHealth services and medical devices	Questionnaire
KPI 8.3	Adoption of the SPHINX Toolkit	Questionnaire
KPI 8.4	Increased use of eHealth and mHealth services and medical devices	Questionnaire

Table 18: Pilot in Portugal: SPHINX Tools Contributing to Applicable Evaluation 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.

5 Planning of Pilot Operations

This section describes the current status of the planning of pilot operations to be performed within the SPHINX Project, involving four pilot sites in Greece, Romania and Portugal. This activity is part of the work developed in Work Package 7 - Technology Validation Pilots and Privacy Assessment.

Aside from Task 7.1 - Sites Surveys and Planning of Pilot Operations, which work is summarised in the present report, WP7 activities involve three other tasks, to be started in August 2020 (month 20):

- Task 7.2 - System Functional Testing and Validation;
- Task 7.3 - Real Life Scenarios & Test Cases Definition;
- Task 7.4 - Legal Analysis Evaluation of the SPHINX Use Cases and Business Model.

Both Tasks 7.2 and 7.3 are directly associated with the integration work being performed in WP6 - SPHINX Common Integration Platform & Incremental Strategy and follow the specifications identified in the deliverable *D6.1 - Specifications of SPHINX Software Integration Framework* [7], as well as the effort related with the implementation of the SPHINX integration infrastructure as part of Tasks 6.2 - Infrastructure and SPHINX Continuous Integration/Development, 6.3 - Big Data Management Infrastructure and SPHINX Analytic Tools and 6.4 - System integration execution, concerning the deliverable *D6.2 - Implementation of the SPHINX Continuous Integration Infrastructure and Big Data Management Infrastructures* to be submitted in October 2020 (month 22). In addition, Task 7.3 benefits directly of the outputs of WP3 – Cyber Security Risk Assessment & Beyond - SPHINX Intelligence to assist the pilots' risk assessment.

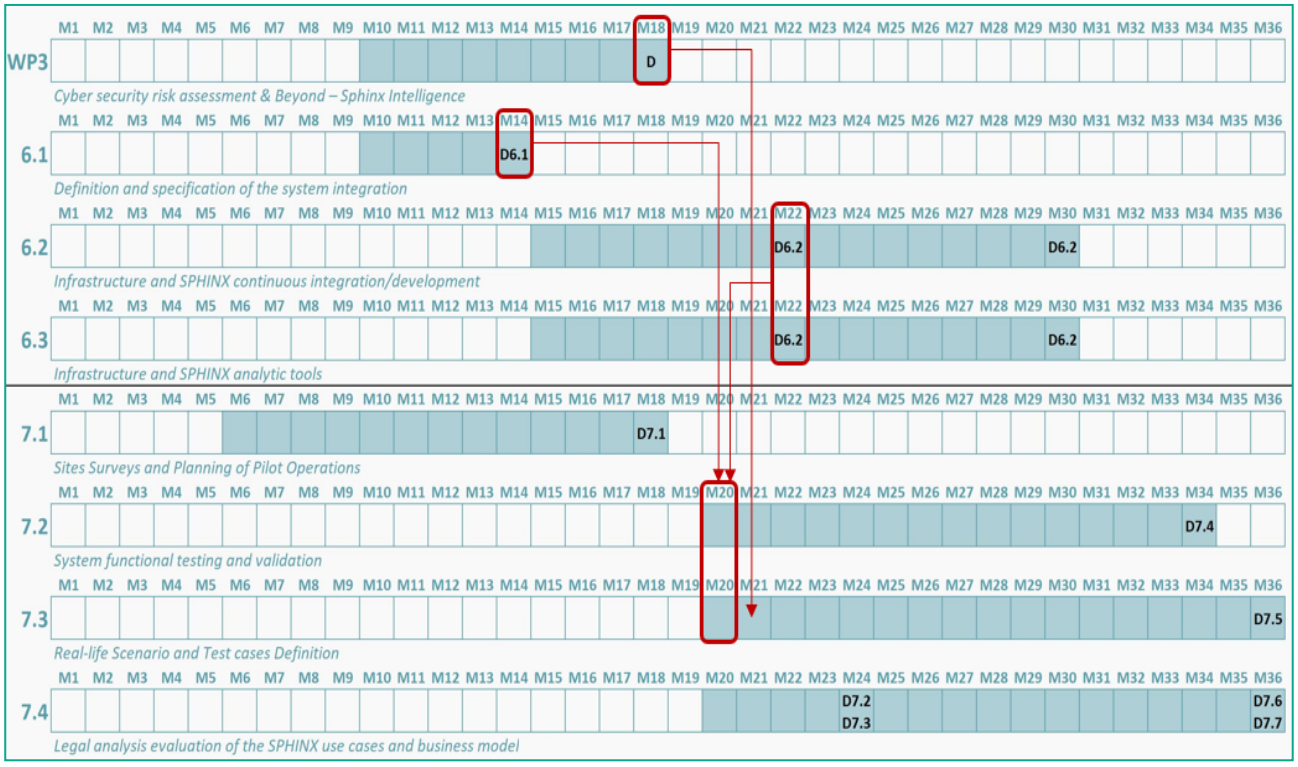

Figure 22: Gantt Chart with WP7 Tasks and Dependencies

Hence, based on the SPHINX Work Plan, it is envisaged that the Pilot Operations may start from August 2020 (month 20), encompassing activities such as the preparation of a realistic environment within the pilot sites where the SPHINX Toolkit will be deployed for validation, after the integration and testing in a lab environment developed in WP6.

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.

Task 7.4 concerns the legal analysis and evaluation of the SPHINX Use Cases and business model and, consequently, depends directly of the outcomes of the previous WP7 tasks, considering important references included in the deliverables *D2.1 - Advanced Cyber Security Threats Digest and Analysis* [6], *D2.4 - Use Cases Definition and Requirements v1* [1], *D2.5 - SPHINX Requirements and Guidelines v1* [2], *D2.6 - SPHINX Architecture v2* [3] and *D6.1 - Specifications of SPHINX Software Integration Framework* [7], as well as the work performed in Tasks T8.5 - Knowledge Management and IPR Protection, T8.2 - Market Analysis and Identification of Customer Segments and T8.3 - Exploitation, Sustainability & Business Plans.

Work Package 7 Workshops

As part of WP 7 activities, the SPHINX Consortium plans to hold three workshops focusing on the SPHINX pilots' results that contribute to the overall SPHINX dissemination strategy:

- Cybersecurity Awareness in Healthcare Employees, Location: Greece;
- The SPHINX Universal Toolkit for Healthcare Organisations, Location: Portugal;
- The Impact of SPHINX in Healthcare Organisations: Pilot Results, Location: Romania.

Due to the COVID-19 situation, and in alignment with current and future safety and public health measures for participants / stakeholders, these workshops may be substituted by specific, online materials prepared by the SPHINX partners on the SPHINX results and the Pilots results, accompanied by live presentation via YouTube streaming. The scheduling for the Workshops is tentatively organised as shown in Table 19. It is noted that this workshop schedule may be finalised within the second half of 2020.

Workshop Title	Location	Date
Cybersecurity Awareness in Healthcare Employees	Greece	4th quarter 2020 or 1st quarter 2021
The SPHINX Universal Toolkit for Healthcare Organisations	Portugal	3rd quarter 2021
The Impact of SPHINX in Healthcare Organisations: Pilot Results	Romania	4th quarter 2021

***Table 19:* WP7 Workshops Schedule**

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 Conclusions

This deliverable reports the outcomes of Task 7.1 - Sites Surveys and Planning of Pilot Operations and addresses in detail the activities to take place in four reference pilot sites in Greece, Romania and Portugal, as part of the planned SPHINX pilots: Pilot in Greece: Intra-Region Patient Data Transfer, Pilot in Greece and Romania: Cross-border Medical Data Exchange and Pilot in Portugal: Securing Advanced Patient Care in Hospital and Homecare Environments. Firstly, the results of the questionnaires implemented by the SPHINX partners to ascertain the level of cybersecurity awareness within the pilot reference sites are presented and analysed, before the deployment and adoption of the SPHINX Toolkit. Then, the pilot operations plan is described, comprising the characterisation of the ICT infrastructure and associated critical assets of the pilot sites and an overview of the planned SPHINX pilot activities, highlighting the involved actors, their roles and responsibilities, the applicable SPHINX use cases and tools and the evaluation framework to serve the assessment of the SPHINX Toolkit's performance and effectiveness concerning cybersecurity events, incidents and attacks. Finally, the planning of the pilot operations announces the scheduled SPHINX Workshops, created to disseminate the SPHINX pilots' outcomes and the SPHINX project results.

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] *D2.4 - Use Cases Definition and Requirements Document v1,* SPHINX Consortium, December 31 2019.

[2] *D2.5 - SPHINX Requirements and Guidelines v1,* SPHINX Consortium, October 10 2019.

[3] *D2.6 - SPHINX Architecture v2*, SPHINX Consortium, February 24 2020.

[4] *ICT Specialists in Employment: Statistics Explained*, Eurostat, 2018, https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_in_employment.

[5] *ENISA Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures*, European Union Agency for Network and Information Security, November 2016.

[6] *D2.1 - Advanced Cyber Security Threats Digest and Analysis,* SPHINX Consortium, September 4 2019.

[7] *D6.1 - Specifications of SPHINX Software Integration Framework,* SPHINX Consortium, February 4 2020.

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.

Annex I: Results of the ICT Questionnaire

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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=28 (100%)	Female n=10 (35,7%)	Male n=18 (64,3%)	20-39 n=9 (32,1%)	40-60 n=19 (67,9%)	Secondary Education n=4 (14,3%)	Vocational training institute n=1 (3,6 %)	Bachelor Degree n=16 (57,1 %)	MSc n=6 (21,4%)	PhD n=1 (3,6%)	0-5 n=4 (14,3%)	6-10 n=3 (10,7%)	>10 n=21 (75 %)	0-1 n=19 (68%)	1,1-2 n=6 (21%)	2,1-3 n=1 (4%)	3,1-4 n=2 (7%)
Usage of Secure method or other methods for third party accesses																	
VPN	14	5	9	4	10	1	1	7	4	1	3	-	11	11	1	1	1
TeamViewer	18	7	11	5	13	3	-	8	6	1	-	3	15	13	5	-	-
AnyDesk	19	7	12	6	13	4	-	7	6	1	1	3	16	14	4	-	1
Remote Desktop	5	2	4	1	4	-	-	4	2	-	-	-	6	4	2	-	-
Other secure method	5	1	1	1	1	-	-	1	-	-	-	1	1	2	1	-	-
Other unsecure method	1	-	1	-	1	-	-	1	-	-	-	-	1	1	-	-	-
Communication ports opened and monitored during daily operations (constantly or on demand)																	
Port TCP 22 (SSH)	8	2	6	3	5	1	-	4	2	1	1	-	7	5	2	-	1
Port TCP 23 (Telnet)	2	-	2	1	1	-	-	2	-	-	-	-	2	-	2	-	-
Port TCP 3389 (RDP)	8	2	6	2	6	1	-	4	3	-	-	--	8	6	2	-	-
Port TCP 20 (FTP data)	4	-	6	3	3	-	1	3	1	1	3	-	3	4	-	1	1
Port TCP 21 (FTP control)	5	-	5	3	2	-	1	4	-	-	3	-	2	3	-	1	1
other	15	8	7	3	12	3	-	7	4	-	-	3	12	11	4	-	-

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.

Do existing SLAs include terms that ensure cybersecurity policies are applied by the external partner for preventing data breaches when connected remotely to hospital's information systems?																	
Yes	6 (21,5%)	2 (20%)	4 (22,2%)	2 (22,2%)	4 (21,0%)	2 (50%)	-	2 (12,5%)	2 (33,3%)	-	1 (25%)	-	5 (23,8%)	5 (26,3%)	-	-	1 (50%)
No	9 (32,1%)	2 (20%)	7 (38,9%)	1 (11,1%)	8 (42,1%)	-	-	5 (31,3%)	3 (50%)	1 (100%)	-	1 (33,3%)	8 (38,1%)	8 (42,1%)	1 (16,7%)	-	-
Do not know	13 (46,4%)	6 (60%)	7 (38,9%)	6 (66,7%)	7 (36,8%)	2 (50%)	1 (100%)	9 (56,2%)	1 (16,7%)	-	3 (75%)	2 (66,6%)	8 (38,1%)	6 (31,6%)	5 (83,3%)	1 (100%)	1 (50%)

Table 20: ICT questionnaires - DYPE5 responses to connection methods & communications ports used and SLA terms

Table 20 contains DYPE5 ICT personnel responses to the following sentences/questions:

- Usage of Secure method or other methods for third party accesses
- Communication ports opened and monitored during daily operations (constantly or on demand)
- Do existing SLAs include terms that ensure cybersecurity policies are applied by the external partner for preventing data breaches when connected remotely to hospital's information 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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=7 (100%)	Female n=1 (14,3%)	Male n=6 (85,7%)	20-39 n=2 (28,6%)	40-60 n=5 (71,4%)	Secondary Education n=3 (42,9%)	Vocational training institute n=1 (14,3%)	Bachelor Degree n=1 (14,3%)	MSc n=2 (28,6%)	PhD n=0 (0%)	0-5 n=0 (0%)	6-10 n = 1 (14,3%)	>10 n=6 (85,7%)	0-1 n=6 (85,7%)	1,1-2 n=1 (14,3%)	2,1-3 n=0 (0%)	3,1-4 n=0 (0%)
Usage of Secure method or other methods for third party accesses																	
VPN	6	1	5	2	4	3	1	1	1	-	-	1	5	5	1	-	-
TeamViewer	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
AnyDesk	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Remote Desktop	1	-	1	1	-	1	-	-	-	-	-	1	-	-	1	-	-
Other secure method	1	-	1	-	-	1	-	-	-	-	-	-	1	1	-	-	-
Other unsecure method	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Communication ports opened and monitored during daily operations (constantly or on demand)																	
Port TCP 22 (SSH)	3	-	3	1	2	2	-	-	1	-	-	1	2	2	1	-	-
Port TCP 23 (Telnet)	1	-	1	1	-	-	1	-	-	-	-	-	1	1	-	-	-
Port TCP 3389 (RDP)	4	1	3	-	4	2	-	1	1	-	-	-	4	4	-	-	-
Port TCP 20 (FTP data)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Port TCP 21 (FTP control)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
other	2	-	2	-	2	1	-	-	1	-	-	-	2	2	-	-	-

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.

Do existing SLAs include terms that ensure cybersecurity policies are applied by the external partner for preventing data breaches when connected remotely to hospital's information systems?																	
Yes	2 (28,6%)	-	2 (33,3%)	-	2 (40%)	1 (33,3%)	-	-	1 (50%)	-	-	-	2 (33,3%)	2 (33,3%)	-	-	-
No	1 (14,3%)	1 (100%)	-	-	1 (20%)	-	-	1 (100%)	-	-	-	-	1 (16,7%)	1 (16,7%)	-	-	-
Do not know	4 (57,1%)	-	4 (66,7%)	2 (100%)	2 (40%)	2 (66,7%)	1 (100%)	-	1 (50%)	-	-	1 (100%)	3 (50%)	3 (50%)	1 (100%)	-	-

Table 21: ICT questionnaires - HESE responses to connection methods & communications ports used and SLA terms

Table 21 contains HESE ICT personnel responses to the following sentences/questions:

- Usage of Secure method or other methods for third party accesses
- Communication ports opened and monitored during daily operations (constantly or on demand)
- Do existing SLAs include terms that ensure cybersecurity policies are applied by the external partner for preventing data breaches when connected remotely to hospital's information 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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n = 2 (100%)	Female n=0 (0%)	Male n=2 (100%)	20-39 n=0 (0%)	40-60 n=2 (100%)	Secondary Education n=0 (0%)	Vocational training institute n=0 (0%)	Bachelor Degree n=1 (50%)	MSc n=1 (50%)	PhD n=0 (0%)	0-5 n=0 (0%)	6-10 n=0 (0%)	>10 n=2 (100%)	0-1 n=2 (100%)	1.1-2 n=0 (0%)	2.1-3 n=0 (0%)	3.1-4 n=0 (0%)
Usage of Secure method or other methods for third party accesses																	
VPN	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
TeamViewer	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
AnyDesk	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Remote Desktop	2	-	2	-	2	-	-	1	1	-	-	-	1	1	-	-	-
Other secure method	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Other unsecure method	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Communication ports opened and monitored during daily operations (constantly or on demand)																	
Port TCP 22 (SSH)	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Port TCP 23 (Telnet)	1	-	1	-	1	-	-	1	-	-	-	-	1	1	-	-	-
Port TCP 3389 (RDP)	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Port TCP 20 (FTP data)	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Port TCP 21 (FTP control)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
other	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

Do existing SLAs include terms that ensure cybersecurity policies are applied by the external partner for preventing data breaches when connected remotely to hospital's information systems?																	
Yes	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
No	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-
Do not know	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 22: ICT questionnaires - POLARIS responses to connection methods & communications ports used and SLA terms

Table 22 contains Polaris ICT personnel responses to the following sentences/questions:

- Usage of Secure method or other methods for third party accesses
- Communication ports opened and monitored during daily operations (constantly or on demand)
- Do existing SLAs include terms that ensure cybersecurity policies are applied by the external partner for preventing data breaches when connected remotely to hospital's information 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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=28 (100%)	Female n=10 (35,7%)	Male n=18 (64,3%)	20-39 n=9 (32,1%)	40-60 n=19 (67,9%)	Secondary Education n=4 (14,3%)	Vocational training institute n=1 (3,6 %)	Bachelor Degree n=16 (57,1 %)	MSc n=6 (21,4%)	PhD n=1 (3,6%)	0-5 n=4 (14,3%)	6-10 n=3 (10,7%)	>10 n=21 (75 %)	0-1 n=19 (68%)	1,1-2 n=6 (21%)	2,1-3 n=1 (4%)	3,1-4 n=2 (7%)
Does your organization have an Official Cybersecurity Plan?																	
Yes	1 (3,57%)	-	1 (5,56%)	1 (11,11%)	-	-	-	1 (6,25%)	-	-	1 (25%)	-	-	-	-	-	1 (50%)
No	4 (14,29%)	9 (90%)	14 (77,78%)	8 (88,89%)	15 (78,95%)	4 (100%)	1 (100%)	12 (75%)	5 (83,33%)	1 (100%)	3 (75%)	3 (100%)	17 (80,95%)	16 (84,21%)	5 (83,33%)	1 (100%)	1 (50%)
Do not know	23 (82,14%)	1 (10%)	3 (16,67%)	-	4 (21,05%)	-	-	3 (18,75%)	1 (16,67%)	-	-	-	4 (19,05%)	3 (15,79%)	1 (16,67%)	-	-
If the previous answer is **yes**. which of the following plans?																	
Risk Assessment	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Incident Respond Plan	1 (100%)	-	1 (100%)	1 (100%)	-	-	-	1 (100%)	-	-	1 (100%)	-	-	-	-	-	1 (100%)
Mitigation plan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Report plan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Have any cybersecurity tests been performed in your Organisation during the last 2 years?																	
Yes	5 (17,86%)	-	5 (27,78%)	3 (33,33%)	2 (10,53%)	-	1 (100%)	4 (25%)	-	-	2 (50%)	-	3 (14,29%)	1 (5,26%)	2 (33,33%)	1 (100%)	1 (50%)
No	23 (82,14%)	10 (100%)	13 (72,22%)	6 (66,67%)	17 (89,47%)	4 (100%)	-	12 (75%)	6 (100%)	1 (100%)	2 (50%)	3 (100%)	18 (85,71%)	18 (94,74%)	4 (66,67%)	-	1 (50%)

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.

If the previous answer is **yes**. which of the following tests? (multiple selection)																	
Scanning	2	-	2	2	-	-	1	1	-	-	2	-	-	-	-	1	1
Penetration	2	-	2	1	1	-	-	2	-	-	1	-	1	1		1	
Weak password identification	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Phishing	3	-	3	2	1	-	1	2	-	-	2	-	1	1	-	1	1
Virus/malware checking	5	-	5	3	2	-	1	4	-	-	2	-	3	1	2	1	1
Verification of latest updates/outdates	2	-	2	1	1	-	-	2	-	-	-	-	2	-	2	-	-
Other	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Are you familiar with the Directive (EU) 2016/1148 NIS Directive and GDPR regulation?																	
Yes	8 (28,57%)	2 (20%)	6 (33,33%)	3 (33,33%)	5 (26,32%)	1 (25%)	-	4 (25%)	2 (33,33%)	1 (100%)	1 (25%)	2 (66,67%)	5 (23,81%)	6 (31,58%)	2 (33,33%)	-	-
No	10 (35,71%)	5 (50%)	5 (27,78%)	2 (22,22%)	8 (42,11%)	2 (50%)	-	6 (37,5%)	2 (33,33%)	-	1 (25%)	-	9 (42,86%)	8 (42,11%)	1 (16,67%)	-	1 (50%)
Partially	10 (35,71%)	3 (30%)	7 (38,89%)	4 (44,44%)	6 (31,58%)	1 (25%)	1 (100%)	6 (37,5%)	2 (33,33%)	-	2 (50%)	1 (33,33%)	7 (33,33%)	5 (26,32%)	3 (50%)	1 (100%)	1 (50%)
Is DDOS attack considered a criminal action according to your National legislation?																	
Yes	10 (35,71%)	1 (10%)	9 (50%)	3 (33,33%)	7 (36,84%)	-	-	7 (43,75%)	2 (33,33%)	1 (100%)	2 (50%)	-	8 (38,10%)	5 (26,32%)	3 (50%)	1 (100%)	1 (50%)
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do not know	18 (64,29%)	9 (90%)	9 (50,00%)	6 (66,67%)	12 (63,16%)	4 (100%)	1 (100%)	9 (56,25%)	4 (66,67%)	-	2 (50%)	3 (100%)	13 (61,90%	14 (73,68%)	3 (50%)	-	1 (50%)

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.

Does your working practice have policies and procedures for the assignment of a unique identifier for each authorized user according to its role?																	
Yes	12 (42,86%)	2 (20%)	10 (55,56%)	5 (55,56%)	7 (36,84%)	1 (25%)	1 (100%)	6 (37,5%)	3 (50%)	1 (100%)	3 (75%)	-	9 (42,86%)	7 (36,84%)	2 (33,33%)	1 (100%)	2 (100%)
No	10 (35,71%)	5 (50%)	5 (27,78%)	3 (33,33%)	7 (36,84%)	1 (25%)	-	6 (37,5%)	3 (50%)	-	-	3 (100%)	7 (33,33%)	8 (42,11%)	2 (33,33%)	-	-
Do not know	6 (21,43%)	3 (30%)	3 (16,67%)	1 (11,11%)	5 (26,32%)	2 (50%)	-	4 (25%)	-	-	1 (25%)	-	5 (23,81%)	4 (21,05%)	2 (33,33%)	-	-
Does your working practice have back up information systems so that it can access HIS in the event of an emergency or when your practice's primary systems become unavailable i.e. in the event of a disaster?																	
Yes	20 (71,43%)	6 (60%)	14 (77,78%)	6 (66,67%)	14 (73,68%)	3 (75%)	1 (100%)	11 (68,75%)	4 (66,67%)	1 (100%)	4 (100%)	-	16 (76,19%)	14 (73,68%)	3 (50%)	1 (100%)	2 (100%)
No	8 (28,57%)	4 (40%)	4 (22,22%)	3 (33,33%)	5 (26,32%)	1 (25%)	-	5 (31,25%)	2 (33,33%)	-	-	3 (100%)	5 (23,81%)	5 (26,32%)	3 (50%)	-	-
Do SSL certificates exist for web-based Hospital Information Systems?																	
Yes	12 (42,86%)	4 (40%)	8 (44,44%)	6 (66,67%)	6 (31,58%)	2 (50%)	1 (100%)	7 (43,75%)	2 (33,33%)	-	3 (75%)	1 (33,33%)	8 (38,10%)	6 (31,58%)	3 (50%)	1 (100%)	2 (100%)
No	9 (32,14%)	1 (10%)	8 (44,44%)	1 (11,11%)	8 (42,11%)	-	-	5 (31,25%)	3 (50,00%)	1 (100%)	1 (25%)	-	8 (38,10%)	9 (47,37%)	-	-	-
Partially	7 (25,00%)	5 (50%)	2 (11,11%)	2 (22,22%)	5 (26,32%)	2 (50%)	-	4 (25%)	1 (16,67%)	-	-	2 (66,67%)	5 (23,81%)	4 (21,05%)	3 (50%)	-	-

Table 23: ICT questionnaires - DYPE5 responses to cybersecurity plans and testing, regulations and legislation knowledge, working practices and SSL certificates existence for HIS

Table 23 contains DYPE5 ICT personnel responses to the following sentences/questions:

- Does your organization have an Official Cybersecurity Plan?
- Have any cybersecurity tests been performed in your Organisation during the last 2 years?
- Are you familiar with the Directive (EU) 2016/1148 NIS Directive and GDPR regulation?
- Is DDOS attack considered a criminal action according to your National legislation?
- Does your working practice have policies and procedures for the assignment of a unique identifier for each authorized user according to its role?
- Does your working practice have back up information systems so that it can access HIS in the event of an emergency or when your practice's primary systems become unavailable i.e. in the event of a disaster?
- Do SSL certificates exist for web-based Hospital Information 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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
Tools used daily for Information Security	**n=28 (100%)**	**Female n=10 (35,7%)**	**Male n=18 (64,3%)**	**20-39 n=9 (32,1%)**	**40-60 n=19 (67,9%)**	**Secondary Education n=4 (14,3%)**	**Vocational training institute n=1 (3,6 %)**	**Bachelor Degree n=16 (57,1 %)**	**MSc n=6 (21,4%)**	**PhD n=1 (3,6%)**	**0-5 n=4 (14,3%)**	**6-10 n=3 (10,7%)**	**>10 n=21 (75 %)**	**0-1 n=19 (68%)**	**1,1-2 n=6 (21%)**	**2,1-3 n=1 (4%)**	**3,1-4 n=2 (7%)**
Access control lists	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Antivirus/malware	26	9	17	8	18	3	1	15	6	1	3	3	20	18	6	-	2
Data encryption (data in transit)	2	-	2	1	1	-	-	1	-	1	1	-	1	1	-	-	1
Firewall(s)	20	7	13	7	13	2	-	13	4	1	2	3	15	14	5	-	1
Intrusion detection systems (IDS)	2	-	2	-	2	-	-	-	2	-	-	-	2	2	-	-	-
Intrusion prevention system	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Mobile device management	1	-	1	-	1	-	-	-	-	1	-	-	1	1	-	-	-
My duties do not include cyber-security activities	2	-	2	1	1	-	-	1	1	-	1	-	1	1	-	1	-
Network monitoring tools	6	1	5	2	4	-	-	5	-	1	-	1	5	3	3	-	-
Patch & vulnerability management	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Single sign on	2	-	2	-	2	-	-	-	2	-	-	-	2	2	-	-	-
User access controls	9	2	7	1	8	2	-	3	3	1	-	-	9	9	-	-	-
Web security gateway	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-

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 loss prevention (DLP application)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Multi-factor authentication	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Messaging security gateway	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 24: ICT questionnaires - DYPE5 responses to information security tools usage

Table 24 contains DYPE5 ICT personnel responses to the following sentences/questions:

- Tools used daily for Information Security

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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=7 (100%)	Female n=1 (14,3%)	Male n=6 (85,7%)	20-39 n=2 (28,6%)	40-60 n=5 (71,4%)	Secondary Education n=3 (42,9%)	Vocational training institute n=1 (14,3%)	Bachelor Degree n=1 (14,3%)	MSc n=2 (28,6%)	PhD n=0 (0%)	0-5 n=0 (0%)	6-10 n=1 (14,3%)	>10 n=6 (85,7%)	0-1 n=6 (85,7%)	1,1-2 n=1 (14,3%)	2,1-3 n=0 (0%)	3,1-4 n=0 (0%)
Does your organization have an Official Cybersecurity Plan?																	
Yes	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No	3 (42,86%)	1 (100%)	2 (33,33%)	-	3 (60%)	1 (33,33%)	-	1 (100%)	1 (50%)	-	-	-	3 (50%)	2 (40%)	-	-	-
Do not know	4 (57,14%)	-	4 (66,67%)	2 (100%)	2 (40%)	2 (66,67%)	1 (100%)	-	1 (50%)	-	-	1 (100%)	3 (50%)	3 (60%)	1 (100%)	-	-
If the previous answer is **yes**. which of the following plans?																	
Risk Assessment	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Incident Respond Plan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Mitigation plan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Report plan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Have any cybersecurity tests been performed in your Organisation during the last 2 years?																	
Yes	4 (57,14%)	-	4 (66,67%)	1 (50%)	3 (60%)	2 (66,67%)	1 (100%)	-	1 (50%)	-	-	-	4 (66,67%)	3 (60%)	-	-	-
No	3 (42,86%)	1 (100%)	2 (33,33%)	1 (50%)	2 (40%)	1 (33,33%)	-	1 (100%)	1 (50%)	-	-	1 (100%)	2 (33,33%)	2 (40%)	1 (100%)	-	-

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.

If the previous answer is **yes**. which of the following tests? (multiple selection)																	
Phishing	2	-	2	1	1	-	1	-	1	-	-	-	2	2	-	-	-
Verification of latest updates/outdates	2	-	2	-	2	1	-	-	1	-	-	-	2	1	-	-	-
Virus/malware checking	3	-	3	-	3	2	-	-	1	-	-	-	3	2	-	-	-
Weak password identification	3	-	3	-	3	2	-	-	1	-	-	-	3	2	-	-	-
Scanning	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Penetration	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Other	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Are you familiar with the Directive (EU) 2016/1148 NIS Directive and GDPR regulation?																	
Yes	1 (14,29%)	-	1 (16,67%)	-	1 (20%)	-	-	-	1 (50%)	-	-	-	1 (16,67%)	1 (20%)	-	-	-
No	3 (42,86%)	-	3 (50%)	2 (100%)	1 (20%)	2 (66,67%)	1 (100%)	-	-	-	-	1 (100%)	2 (33,33%)	2 (40%)	1 (100%)	-	-
Partially	3 (42,86%)	1 (100%)	2 (33,33%)	-	3 (60%)	1 (33,33%)	-	1 (100%)	1 (50%)	-	-	-	3 (50%)	2 (40%)	-	-	-
Is DDOS attack considered a criminal action according to your National legislation?																	
Yes	7 (100%)	1 (100%)	6 (100%)	2 (100%)	5 (100%)	3 (100%)	1 (100%)	1 (100%)	2 (100%)	-	-	1 (100%)	6 (100%)	5 (100%)	1 (100%)	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do not know	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

Does your working practice have policies and procedures for the assignment of a unique identifier for each authorized user according to its role?																	
Yes	4	1	3	-	4	1	-	1	2	-	-	-	4	3	-	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do not know	2	-	2	1	1	2	-	-	-	-	-	1	1	1	1	-	-
Does your working practice have back up information systems so that it can access HIS in the event of an emergency or when your practice's primary systems become unavailable i.e. in the event of a disaster?																	
Yes	6 (85,71%)	1 (100%)	5 (83,33%)	2 (100%)	4 (80%)	3 (100%)	1 (100%)	1 (100%)	1 (50%)	-	-	1 (100%)	5 (83,33%)	4 (80%)	1 (100%)	-	-
No	1 (14,29%)	-	1 (16,67%)	-	1 (20%)	-	-	-	1 (50%)	-	-	-	1 (16,67%)	1 (20%)	-	-	-
Do SSL certificates exist for web-based Hospital Information Systems?																	
Yes	4 (57,14%)	-	4 (66,67%)	2 (100%)	2 (40%)	2 (66,67%)	1 (100%)	-	1 (50%)	-	-	1 (100%)	3 (50%)	3 (60%)	1 (100%)	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Partially	3 (42,86%)	1 (100%)	2 (33,33%)	-	3 (60%)	1 (33,33%)	-	1 (100%)	1 (50%)	-	-	-	3 (50%)	2 (40%)	-	-	-

Table 25: ICT questionnaires - HESE responses to cybersecurity plans and testing, regulations and legislation knowledge, working practices, SSL certificates existence for HIS

Table 25 contains HESE ICT personnel responses to the following sentences/questions:

- Does your organization have an Official Cybersecurity Plan?
- Have any cybersecurity tests been performed in your Organisation during the last 2 years?
- Are you familiar with the Directive (EU) 2016/1148 NIS Directive and GDPR regulation?
- Is DDOS attack considered a criminal action according to your National legislation?
- Does your working practice have policies and procedures for the assignment of a unique identifier for each authorized user according to its role?
- Does your working practice have back up information systems so that it can access HIS in the event of an emergency or when your practice's primary systems become unavailable i.e. in the event of a disaster?
- Do SSL certificates exist for web-based Hospital Information 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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
Tools used daily for Information Security	**n=7 (100%)**	**Female n=1 (14,3%)**	**Male n=6 (85,7%)**	**20-39 n=2 (28,6%)**	**40-60 n=5 (71,4%)**	**Secondary Education n=3 (42,9%)**	**Vocational training institute n=1 (14,3%)**	**Bachelor Degree n=1 (14,3%)**	**MSc n=2 (28,6%)**	**PhD n=0 (0%)**	**0-5 n=0 (0%)**	**6-10 n=1 (14,3%)**	**>10 n=6 (85,7%)**	**0-1 n=6 (85,7%)**	**1,1-2 n=1 (14,3%)**	**2,1-3 n=0 (0%)**	**3,1-4 n=0 (0%)**
Access control lists	2	-	2	-	2	1	-	-	1	-	-	-	2	2	-	-	-
Antivirus/malware	7	1	6	2	5	3	1	1	2	-	-	1	6	5	1	-	-
Data encryption (data in transit)	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Firewall(s)	3	-	3	1	2	2	-	-	1	-	-	1	2	1	1	-	-
Multi-factor authentication	2	-	2	-	2	1	-	-	1	-	-	-	2	2	-	-	-
Network monitoring tools	4	-	4	1	3	3	-	-	1	-	-	1	3	2	1	-	-
Patch & vulnerability management	1	-	1	-	1	1	-	-	-	-	-	-	1	1	-	-	-
User access controls	4	-	4	1	3	3	-	-	1	-	-	1	3	2	1	-	-
Access control lists	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Web security gateway	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Data loss prevention (DLP application)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Audit logs of each access to pt. health 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.

financial records																	
My duties do not include cyber-security activities	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Data encryption (data at rest)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Intrusion detection systems (IDS)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Mobile device management	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Intrusion prevention system	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Single sign on	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Messaging security gateway	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 26: ICT questionnaires - HESE responses to information security tools usage

Table 26 contains HESE ICT personnel responses to the following sentences/questions:

- Tools used daily for Information Security

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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=2 (100%)	Female n=0 (0%)	Male n=2 (100%)	20-39 n=0 (0%)	40-60 n=2 (100%)	Secondary Education n=0 (0%)	Vocational training institute n=0 (0%)	Bachelor Degree n=1 (50%)	MSc n=1 (50%)	PhD n=0 (0%)	0-5 n=0 (0%)	6-10 n=0 (0%)	>10 n=2 (100%)	0-1 n=2 (100%)	1.1-2 n=0 (0%)	2.1-3 n=0 (0%)	3.1-4 n=0 (0%)
Does your organization have an Official Cybersecurity Plan?																	
Yes	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
No	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-
Do not know	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
If the previous answer is **yes**. which of the following plans?																	
Risk Assessment	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Incident Respond Plan	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Mitigation plan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Report plan	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Have any cybersecurity tests been performed in your Organisation during the last 2 years?																	
Yes	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
No	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-

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.

If the previous answer is **yes**. which of the following tests? (multiple selection)																	
Scanning	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Penetration	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Weak password identification	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Phishing	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Virus/malware checking	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Verification of latest updates/outdates	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Other	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Are you familiar with the Directive (EU) 2016/1148 NIS Directive and GDPR regulation?																	
Yes	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Partially	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-
Is DDOS attack considered a criminal action according to your National legislation?																	
Yes	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do not know	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-

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.

Does your working practice have policies and procedures for the assignment of a unique identifier for each authorized user according to its role?																	
Yes	2 (100%)	-	2 (100%)	-	2 (100%)	-	-	1 (100%)	1 (100%)	-	-	-	2 (100%)	2 (100%)	-	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do not know	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Does your working practice have back up information systems so that it can access HIS in the event of an emergency or when your practice's primary systems become unavailable i.e. in the event of a disaster?																	
Yes	2 (100%)	-	2 (100%)	-	2 (100%)	-	-	1 (100%)	1 (100%)	-	-	-	2 (100%)	2 (100%)	-	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do SSL certificates exist for web-based Hospital Information Systems?																	
Yes	2 (100%)	-	2 (100%)	-	2 (100%)	-	-	1 (100%)	1 (100%)	-	-	-	2 (100%)	2 (100%)	-	-	-
No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Partially	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 27: ICT questionnaires - POLARIS responses to cybersecurity plans and testing, regulations and legislation knowledge, working practices, SSL certificates existence for HIS

Table 27 contains Polaris ICT personnel responses to the following sentences/questions:

- Does your organization have an Official Cybersecurity Plan?
- Have any cybersecurity tests been performed in your Organisation during the last 2 years?
- Are you familiar with the Directive (EU) 2016/1148 NIS Directive and GDPR regulation?
- Is DDOS attack considered a criminal action according to your National legislation?
- Does your working practice have policies and procedures for the assignment of a unique identifier for each authorized user according to its role?
- Does your working practice have back up information systems so that it can access HIS in the event of an emergency or when your practice's primary systems become unavailable i.e. in the event of a disaster?
- Do SSL certificates exist for web-based Hospital Information 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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
Tools used daily for Information Security	**n=2 (100%)**	**Female n=0 (0%)**	**Male n=2 (100%)**	**20-39 n=0 (0%)**	**40-60 n=2 (100%)**	**Secondary Education n=0 (0%)**	**Vocational training institute n=0 (0%)**	**Bachelor Degree n=1 (50%)**	**MSc n=1 (50%)**	**PhD n=0 (0%)**	**0-5 n=0 (0%)**	**6-10 n=0 (0%)**	**>10 n=2 (100%)**	**0-1 n=2 (100%)**	**1.1-2 n=0 (0%)**	**2.1-3 n=0 (0%)**	**3.1-4 n=0 (0%)**
Antivirus/malware	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Firewall(s)	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Data encryption (data in transit)	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Data encryption (data at rest)	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Patch & vulnerability management	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Intrusion detection systems (IDS)	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Network monitoring tools	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Mobile device management	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
User access controls	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Intrusion prevention system	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Access control lists	2	-	2	-	2	-	-	1	1	-	-	-	2	2	-	-	-
Single sign on	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Web security gateway	1	-	1	-	1	-	-	-	1	-	-	-	1	1	-	-	-
Data loss prevention (DLP application)	1	-	1	-	1	-	-	1	-	-	-	-	1	1	-	-	-

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.

Audit logs of each access to pt. health and financial records	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
My duties do not include cyber-security activities	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Multi-factor authentication	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Messaging security gateway	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 28: ICT questionnaires - POLARIS responses to information security tools usage

Table 28 contains Polaris ICT personnel responses to the following sentences/questions:

- Tools used daily for Information Security

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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=28 (100%)	Female n=10 (35,7%)	Male n=18 (64,3%)	20-39 n=9 (32,1%)	40-60 n=19 (67,9%)	Secondary Education n=4 (14,3%)	Vocational training institute n=1 (3,6 %)	Bachelor Degree n=16 (57,1 %)	MSc n=6 (21,4%)	PhD n=1 (3,6%)	0-5 n=4 (14,3%)	6-10 n=3 (10,7%)	>10 n=21 (75 %)	0-1 n=19 (68%)	1,1-2 n=6 (21%)	2,1-3 n=1 (4%)	3,1-4 n=2 (7%)
Percentage of Legacy (unsupported) or known vulnerable systems in place (e.g. end of life operating systems in medical devices) in total equipment (%)																	
0-10	8 (28,6%)	3 (30%)	5 (27,8%)	5 (55,6%)	3 (15,8%)	1 (25%)	-	6 (37,5%)	-	1 (100%)	1 (25%)	3 (100%)	4 (19,0%)	3 (15,8%)	4 (66,7%)	-	1 (50%)
11-20	1 (3,6%)	-	1 (5,6%)	-	1 (5,3%)	-	-	-	1 (16,7%)	-	-	-	1 (4,8%)	1 (5,3%)	-	-	-
21-30	4 (14,3%)	1 (10%)	3 (16,7%)	1 (11,1%)	3 (15,8%)	-	1 (100%)	1 (6,3%)	2 (33,3%)	-	1 (25%)	-	3 (14,3%)	3 (15,8%)	-	-	1 (50%)
31-40	1 (3,6%)	1 (10%)	-	-	1 (5,3%)	-	-	1 (6,3%)	-	-	-	-	1 (4,8%)	-	1 (16,7%)	-	-
41-50	1 (3,6%)	-	1 (5,6%)	-	1 (5,3%)	-	-	-	1 (16,7%)	-	-	-	1 (4,8%)	1 (5,3%)	-	-	-
51-60	2 (7,1%)	2 (20%)	-	-	2 (10,5%)	1 (25%)	-	1 (6,3%)	-	-	-	-	2 (9,5%)	2 (10,5%)	-	-	-
More than 60	8 (28,6%)	3 (30%)	5 (27,8%)	1 (11,1%)	7 (36,8%)	-	-	3 (18,8%)	-	-	2 (50%)	-	1 (4,8%)	2 (10,5%)	-	1 (100%)	-
Do not know	3 (10,7%)	-	3 (16,7%)	2 (22,2%)	1 (5,3%)	2 (50%)	-	4 (25,0%)	2 (33,3%)	-	-	-	8 (38,1%)	7 (36,8%)	1 (16,7%)	-	-
Number of cyber security Incidents during the last 3 years (e.g. phishing attacks, virus infections, etc.)?																	
0-5	13 (46,4%)	3 (30%)	10 (55,6%)	5 (55,6%)	8 (42,1%)	2 (50%)	-	8 (50%)	3 (50%)	-	2 (50%)	1 (33,3%)	10 (47,6%)	9 (47,4%)	3 (50%)	-	1 (50%)
6-10	3 (10,7%)	-	3 (16,7%)	1 (11,1%)	2 (10,5%)	-	1 (100%)	1 (6,3%)	-	1 (100%)	1 (25%)	-	2 (9,5%)	2 (10,5%)	-	-	1 (50%)
11-15	1 (3,6%)	-	1 (5,6%)	-	1 (5,3%)	-	-	-	1 (16,7%)	-	-	-	1 (4,8%)	1 (5,3%)	-	-	-
16-20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

21-25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26-30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	11 (39,3%)	7 (70,0%)	4 (22,2%)	3 (33,3%)	8 (42,1%)	2 (50%)	-	7 (43,8%)	2 (33,3%)	-	1 (25%)	2 (66,7%)	8 (38,1%)	7 (36,8%)	3 (50%)	1 (100%)	-
Number of unauthorized login attempts in HIS, Active Directory, RIS/PACS per month?																	
0-5	6 (21,4%)	-	6 (33,3%)	4 (44,4%)	2 (10,5%)	-	-	6 (37,5%)	-	-	2 (50%)	1 (33,3%)	3 (14,3%)	3 (15,8%)	2 (33,3%)	-	1 (50%)
6-10	1 (3,6%)	-	1 (5,6%)	1 (11,1%)	-	-	1 (100%)	-	-	-	1 (25%)	-	-	-	-	-	1 (50%)
11-15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16-20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21-25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26-30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	19 (67,9%)	9 (90%)	9 (50%)	3 (33,3%)	15 (78,9%)	4 (100%)	-	8 (50%)	5 (83,3%)	1 (100%)	-	2 (66,7%)	16 (76,2%)	15 (78,9%)	3 (50%)	-	-
No records kept but it is monitored regularly	3 (10,7%)	1 (10%)	2 (11,1%)	1 (11,1%)	2 (10,5%)	-	-	2 (12,5%)	1 (16,7%)	-	1 (25%)	-	2 (9,5%)	1 (5,3%)	1 (16,7%)	1 (100%)	-
Mean Time to Resolve an Incident?																	
0-6 hours	9 (32,1%)	1 (10%)	8 (44,4%)	5 (55,6%)	4 (21,1%)	-	1 (100%)	8 (50%)	-	-	4 (100%)	1 (33,3%)	4 (19,0%)	5 (26,3%)	1 (16,7%)	1 (100%)	2 (100%)
7-12 hours	1 (3,6%)	1 (10%)	-	-	1 (5,3%)	1 (25%)	-	-	-	-	-	-	1 (4,8%)	1 (5,3%)	-	-	-
13-24 hours	1 (3,6%)	-	1 (5,6%)	-	1 (5,3%)	-	-	-	1 (16,7%)	-	-	-	1 (4,8%)	1 (5,3%)	-	-	-
25-48 hours	4 (14,3%)	2 (20%)	2 (11,1%)	1 (11,1%)	3 (15,8%)	1 (25%)	-	1 (6,3%)	2 (33,3%)	-	-	-	4 (19,0%)	4 (21,1%)	-	-	-
3-7 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.

more than a week	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	13 (46,4%)	6 (60%)	7 (38,9%)	3 (33,3%)	10 (52,6%)	2 (50%)	-	7 (43,8%)	3 (50%)	1 (100%)	-	2 (66,7%)	11 (52,4%)	8 (42,1%)	5 (83,3%)	-	-
Mean Downtime During an Incident?																	
0-6 hours	9 (32,1%)	2 (20%)	7 (38,9%)	5 (55,6%)	4 (21,1%)	-	1 (100%)	7 (43,8%)	1 (16,7%)	-	4 (100%)	1 (33,3%)	4 (19,0%)	5 (26,3%)	1 (16,7%)	1 (100%)	2 (100%)
7-12 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13-24 hours	1 (3,6%)	-	1 (5,6%)	-	1 (5,3%)	-	-	-	1 (16,7%)	-	-	-	1 (4,8%)	1 (5,3%)	-	-	-
25-48 hours	5 (17,9%)	3 (30%)	2 (11,1%)	1 (11,1%)	4 (21,1%)	1 (25,0%)	-	2 (12,5%)	2 (33,3%)	-	-	-	5 (23,8%)	5 (26,3%)	-	-	-
3-7 days	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	13 (46,4%)	5 (50%)	8 (44,4%)	3 (33,3%)	10 (52,6%)	3 (75,0%)	-	7 (43,8%)	2 (33,3%)	1 (100%)	-	2 (66,7%)	11 (52,4%)	8 (42,1%)	5 (83,3%)	-	-

Table 29: ICT questionnaires - DYPE5 responses to legacy systems existence and cybersecurity performance indicators

Table 29 contains DYPE5 ICT personnel responses to the following sentences/questions:

- Percentage of Legacy (unsupported) or known vulnerable systems in place (e.g. end of life operating systems in medical devices) in total equipment (%)
- Number of cyber security Incidents during the last 3 years (e.g. phishing attacks, virus infections, etc.)?
- Number of unauthorized login attempts in HIS, Active Directory, RIS/PACS per month?
- Mean Time to Resolve an Incident?
- Mean Downtime During an Incident?

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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=7 (100%)	Female n=1 (14,3%)	Male n=6 (85,7%)	20-39 n=2 (28,6%)	40-60 n=5 (71,4%)	Secondary Education n=3 (42,9%)	Vocational training institute n=1 (14,3%)	Bachelor Degree n=1 (14,3%)	MSc n=2 (28,6%)	PhD n=0 (0%)	0-5 n=0 (0%)	6-10 n=1 (14,3%)	>10 n=6 (85,7%)	0-1 n=6 (85,7%)	1,1-2 n=1 (14,3%)	2,1-3 n=0 (0%)	3,1-4 n=0 (0%)
Percentage of Legacy (unsupported) or known vulnerable systems in place (e.g. end of life operating systems in medical devices) in total equipment (%)																	
0-10	2 (28,6%)	-	2 (33,3%)	1 (50%)	1 (20%)	2 (66,7%)	-	-	-	-	-	1 (100%)	1 (16,7%)	1 (16,7%)	1 (100%)	-	-
11-20	2 (28,6%)	1 (100%)	1 (16,7%)	-	2 (40%)	-	-	1 (100%)	1 (50%)	-	-	-	2 (33,3%)	2 (33,3%)	-	-	-
21-30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
31-40	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
41-50	1 (14,3%)	-	1 (16,7%)	1 (50%)	-	-	1 (100%)	-	-	-	-	-	1 (16,7%)	1 (16,7%)	-	-	-
51-60	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
More than 60	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do not know	2 (28,6%)	-	2 (33,3%)	-	2 (40%)	1 (33,3%)	-	-	1 (50%)	-	-	-	2 (33,3%)	2 (33,3%)	-	-	-
Number of cyber security Incidents during the last 3 years (e.g. phishing attacks, virus infections, etc.)?																	
0-5	2 (28,6%)	-	2 (33,3%)	1 (50%)	1 (20%)	2 (66,7%)	-	-	-	-	-	1 (100%)	1 (16,7%)	1 (16,7%)	1 (100%)	-	-
6-10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11-15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16-20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

21-25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26-30	1 (14,3%)	-	1 (16,7%)	1 (50%)	-	-	1 (100%)	-	-	-		-	1 (16,7%)	1 (16,7%)	-	-	-
No records kept	4 (57,1%)	1 (100%)	3 (50%)	-	4 (80%)	1 (33,3%)	-	1 (100%)	2 (100%)	-	-	-	4 (66,7%)	4 (66,7%)	-	-	-
Number of unauthorized login attempts in HIS, Active Directory, RIS/PACS per month?																	
0-5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6-10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11-15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16-20	1 (14,3%)	-	1 (16,7%)	1 (50%)	-	-	1 (100%)	-	-	-	-	-	1 (16,7%)	1 (16,7%)	-	-	-
21-25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26-30	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-
No records kept	4 (57,1%)	1 (100%)	3 (50%)	-	4 (80%)	2 (66,7%)	-	1 (100%)	1 (50%)	-	-	-	4 (66,7%)	4 (66,7%)	-	-	-
No records kept but it is monitored regularly	2 (28,6%)	-	-	1 (50%)	1 (20%)	1 (33,3%)	-	-	1 (50%)	-	-	1 (100%)	1 (16,7%)	1 (16,7%)	1 (100%)	-	-
Mean Time to Resolve an Incident?																	
0-6 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7-12 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13-24 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
25-48 hours	1 (14,3%)	-	1 (16,7%)	1 (50%)	-	-	1 (100%)	-	-	-	-	-	1 (16,7%)	1 (16,7%)	-	-	-
3-7 days	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
more than a week	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

No records kept	6 (85,7%)	1 (100%)	5 (83,3%)	1 (50%)	5 (100%)	3 (100%)	-	1 (100%)	2 (100%)	-	-	1 (100%)	5 (83,3%)	5 (83,3%)	1 (100%)	-	-
Mean Downtime During an Incident?																	
0-6 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7-12 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13-24 hours	1 (14,3%)	-	1 (16,7%)	1 (50%)	-	-	1 (100%)	-	-	-	-	-	1 (16,7%)	1 (16,7%)	-	-	-
25-48 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3-7 days	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	6 (85,7%)	1 (100%)	5 (83,3%)	1 (50%)	5 (100%)	3 (100%)	-	1 (100%)	2 (100%)	-	-	1 (100%)	5 (83,3%)	5 (83,3%)	1 (100%)	-	-

Table 30: ICT questionnaires - HESE responses to legacy systems existence and cybersecurity performance indicators

Table 30 contains HESE ICT personnel responses to the following sentences/questions:

- Percentage of Legacy (unsupported) or known vulnerable systems in place (e.g. end of life operating systems in medical devices) in total equipment (%)
- Number of cyber security Incidents during the last 3 years (e.g. phishing attacks, virus infections, etc.)?
- Number of unauthorized login attempts in HIS, Active Directory, RIS/PACS per month?
- Mean Time to Resolve an Incident?
- Mean Downtime During an Incident?

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.

	Total	Gender		Age		Education					Years of experience			Proportion of ICT employees in total employment (%)			
	n=2 (100%)	Female n=0 (0%)	Male n=2 (100%)	20-39 n=0 (0%)	40-60 n=2 (100%)	Secondary Education n=0 (0%)	Vocational training institute n=0 (0%)	Bachelor Degree n=1 (50%)	MSc n=1 (50%)	PhD n=0 (0%)	0-5 n=0 (0%)	6-10 n=0 (0%)	>10 n=2 (100%)	0-1 n=2 (100%)	1.1-2 n=0 (0%)	2.1-3 n=0 (0%)	3.1-4 n=0 (0%)
Percentage of Legacy (unsupported) or known vulnerable systems in place (e.g. end of life operating systems in medical devices) in total equipment (%)																	
0-10	2 (100%)	-	2 (100%)	-	2 (100%)	-	-	1 (100%)	1 (100%)	-	-		2 (100%)	2 (100%)	-	-	-
11-20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21-30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
31-40	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
41-50	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
51-60	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
More than 60	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Do not know	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Number of cyber security Incidents during the last 3 years (e.g. phishing attacks, virus infections, etc.)?																	
0-5	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
6-10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11-15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16-20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

21-25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26-30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-
Number of unauthorized login attempts in HIS, Active Directory, RIS/PACS per month?																	
0-5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6-10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11-15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16-20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21-25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26-30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept but it is monitored regularly	2 (100%)	-	2 (100%)	-	2 (100%)	-	-	1 (100%)	1 (100%)	-	-	-	2 (100%)	2 (100%)	-	-	-
Mean Time to Resolve an Incident?																	
0-6 hours	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
7-12 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13-24 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
25-48 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3-7 days	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
more than a week	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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.

No records kept	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-
Mean Downtime During an Incident?																	
0-6 hours	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	-	1 (100%)	-	-	-	1 (50%)	1 (50%)	-	-	-
7-12 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13-24 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
25-48 hours	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3-7 days	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
No records kept	1 (50%)	-	1 (50%)	-	1 (50%)	-	-	1 (100%)	-	-	-	-	1 (50%)	1 (50%)	-	-	-

Table 31: ICT questionnaires - POLARIS responses to legacy systems existence and cybersecurity performance indicators

Table 31 contains Polaris ICT personnel responses to the following sentences/questions:

- Percentage of Legacy (unsupported) or known vulnerable systems in place (e.g. end of life operating systems in medical devices) in total equipment (%)
- Number of cyber security Incidents during the last 3 years (e.g. phishing attacks, virus infections, etc.)?
- Number of unauthorized login attempts in HIS, Active Directory, RIS/PACS per month?
- Mean Time to Resolve an Incident?
- Mean Downtime During an Incident?

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.

Annex II: Results of the Non-ICT Questionnaire

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
Does your hospital have a Cyber-Security Department or external services?																				
Yes	60 (13,4%)	43 (12,8%)	17 (15,2%)	5 (15,2%)	15 (16,5%)	20 (11,7%)	17 (12,7%)	3 (15%)	8 (12,7%)	5 (15,6%)	30 (12,1%)	17 (18,1%)	-	10 (11,4%)	15 (9,6%)	2 (40%)	4 (12,1%)	22 (17,3%)	1 (11,1%)	6 (19,4%)
No	94 (20,9%)	66 (19,6%)	28 (25%)	5 (15,2%)	13 (14,3%)	40 (23,4%)	29 (21,6%)	7 (35%)	13 (20,6%)	10 (31,3%)	51 (20,6%)	17 (18,1%)	3 (23,1%)	13 (14,8%)	34 (21,8%)	-	7 (21,2%)	32 (25,2%)	1 (11,1%)	7 (22,6%)
Do not know	295 (65,7%)	228 (67,7%)	67 (59,8%)	23 (69,7%)	63 (69,2%)	111 (64,9%)	88 (65,7%)	10 (50%)	42 (66,7%)	17 (53,1%)	166 (67,2%)	60 (63,8%)	10 (76,9%)	65 (73,9%)	107 (68,6%)	3 (60%)	22 (66,7%)	73 (57,5%)	7 (77,8%)	18 (58,1%)
Does your work on the hospital involves working on a computer at any time?																				
Yes	420 (93,5%)	314 (93,2%)	106 (94,6%)	33 (100%)	89 (97,8%)	155 (90,6%)	124 (92,5%)	19 (95%)	54 (85,7%)	24 (75%)	238 (96,4%)	91 (96,8%)	13 (100%)	87 (98,9%)	142 (91%)	3 (60%)	26 (78,8%)	124 (97,6%)	9 (100%)	29 (93,5%)
No	29 (6,5%)	23 (6,8%)	6 (5,4%)	-	2 (2,2%)	16 (9,4%)	10 (7,5%)	1 (5%)	9 (14,3%)	8 (25%)	9 (3,6%)	3 (3,2%)	-	1 (1,1%)	14 (9%)	2 (40%)	7 (21,2%)	3 (2,4%)	-	2 (6,5%)
Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?																				
Yes	138 (30,7%)	101 (30%)	37 (33%)	12 (36,4%)	30 (33%)	45 (26,3%)	43 (32,1%)	8 (40%)	20 (31,7%)	7 (21,9%)	78 (31,6%)	30 (31,9%)	3 (23,1%)	26 (29,5%)	40 (25,6%)	2 (40%)	8 (24,2%)	46 (36,2%)	1 (11,1%)	15 (48,4%)
No	311 (69,3%)	236 (70%)	75 (67%)	21 (63,6%)	61 (67%)	126 (73,7%)	91 (67,9%)	12 (60%)	43 (68,3%)	25 (78,1%)	169 (68,4%)	64 (68,1%)	10 (76,9%)	62 (70,5%)	116 (74,4%)	3 (60%)	25 (75,8%)	81 (63,8%)	8 (88,9%)	16 (51,6%)

Table 32: Non-ICT questionnaires - DYPE5 responses to cyber security support services existence, number of computer related job positions and GDPR training

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 32 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- Does your hospital have a Cyber-Security Department or external services?
- Does your work on the hospital involves working on a computer at any time?
- Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?

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.

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
Does your work in the hospital involves access to patient data, which is considered confidential and sensitive information?																				
Yes	305 (67,9%)	233 (69,1%)	72 (64,3%)	28 (84,8%)	69 (75,8%)	116 (67,8%)	81 (60,4%)	11 (55%)	37 (58,7%)	21 (65,6%)	167 (67,6%)	70 (74,5%)	10 (76,9%)	75 (85,2%)	102 (65,4%)	3 (60%)	25 (75,8%)	72 (56,7%)	1 (11,1%)	27 (87,1%)
No	144 (32,1%)	104 (30,9%)	40 (35,7%)	5 (15,2%)	22 (24,2%)	55 (32,2%)	53 (39,6%)	9 (45%)	26 (41,3%)	11 (34,4%)	80 (32,4%)	24 (25,5%)	3 (23,1%)	13 (14,8%)	54 (34,6%)	2 (40%)	8 (24,2%)	55 (43,3%)	8 (88,9%)	4 (12,9%)
Do you have cyber-security policies at your hospital?																				
Yes	48 (10,7%)	36 (10,7%)	12 (10,7%)	1 (3%)	15 (16,5%)	18 (10,5%)	12 (9%)	2 (10%)	2 (3,2%)	6 (18,8%)	22 (8,9%)	18 (19,1%)	-	8 (9,1%)	10 (6,4%)	-	5 (15,2%)	19 (15%)	1 (11,1%)	5 (16,1%)
No	64 (14,3%)	44 (13,1%)	20 (17,9%)	3 (9,1%)	11 (12,1%)	28 (16,4%)	19 (14,2%)	3 (15%)	7 (11,1%)	9 (28,1%)	33 (13,4%)	11 (11,7%)	4 (30,8%)	9 (10,2%)	17 (10,9%)	1 (20%)	7 (21,2%)	22 (17,3%)	1 (11,1%)	7 (22,6%)
Do not know	337 (75,1%)	257 (76,3%)	80 (71,4%)	29 (87,9%)	65 (71,4%)	125 (73,1%)	103 (76,9%)	15 (75%)	54 (85,7%)	17 (53,1%)	192 (77,7%)	65 (69,1%)	9 (69,2%)	71 (80,7%)	129 (82,7%)	4 (80%)	21 (63,6%)	86 (67,7%)	7 (77,8%)	19 (61,3%)

Table 33: Non-ICT questionnaires - DYPE5 responses to patient data access and cyber security policies existence

Table 33 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- Does your work in the hospital involves access to patient data, which is considered confidential and sensitive information?
- Do you have cyber-security policies at your 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.

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
Do you know when your computer is hacked or infected, and whom to contact when it occurs?																				
Yes, I know when my computer is hacked or infected and I know whom to contact.	143 (31,8%)	104 (30,9%)	39 (34,8%)	8 (24,2%)	34 (37,4%)	58 (33,9%)	34 (25,4%)	9 (45%)	13 (20,6%)	7 (21,9%)	91 (36,8%)	28 (29,8%)	4 (30,8%)	27 (30,7%)	53 (34%)	2 (40%)	8 (24,2%)	40 (31,5%)	3 (33,3%)	10 (32,3%)
No, I do not know when my computer is hacked or infected and I don't know whom to contact.	86 (19,2%)	60 (17,8%)	26 (23,2%)	9 (27,3%)	11 (12,1%)	35 (20,5%)	27 (20,1%)	4 (20%)	17 (27%)	9 (28,1%)	45 (18,2%)	14 (14,9%)	1 (7,7%)	24 (27,3%)	32 (20,5%)	2 (40%)	7 (21,2%)	15 (11,8%)	-	6 (19,4%)
Yes, I know when my computer is hacked or infected but I don't know whom to contact	35 (7,8%)	27 (8%)	8 (7,1%)	4 (12,1%)	6 (6,6%)	17 (9,9%)	8 (6%)	-	5 (7,9%)	3 (9,4%)	16 (6,5%)	10 (10,6%)	1 (7,7%)	12 (13,6%)	13 (8,3%)	-	4 (12,1%)	4 (3,1%)	-	2 (6,5%)
No, I do not know when my computer and I	185 (41,2%)	146 (43,3%)	39 (34,8%)	12 (36,4%)	40 (44%)	61 (35,7%)	65 (48,5%)	7 (35%)	28 (44,4%)	13 (40,6%)	95 (38,5%)	42 (44,7%)	7 (53,8%)	25 (28,4%)	58 (37,2%)	1 (20%)	14 (42,4%)	68 (53,5%)	6 (66,7%)	13 (41,9%)

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.

know whom to contact.																			

Table 34: Non-ICT questionnaires - DYPE5 responses to acknowledge of hacked or infected computer

Table 34 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- Do you know when your computer is hacked or infected, and whom to contact when it occurs?

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.

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
Have you ever found a virus or Trojan on your computer at work?																				
Yes, my computer has been infected before	100 (22,3%)	74 (22%)	26 (23,2%)	6 (18,2%)	16 (17,6%)	43 (25,1%)	29 (21,6%)	6 (30%)	14 (22,2%)	7 (21,9%)	61 (24,7%)	18 (19,1%)	-	17 (19,3%)	42 (26,9%)	-	6 (18,2%)	29 (22,8%)	3 (33,3%)	3 (9,7%)
No, my computer has never been infected	247 (55,0%)	176 (52,2%)	71 (63,4%)	21 (63,6%)	59 (64,8%)	94 (55%)	63 (47%)	10 (50%)	31 (49,2%)	12 (37,5%)	131 (53%)	61 (64,9%)	12 (92,3%)	59 (67%)	74 (47,4%)	2 (40%)	14 (42,4%)	73 (57,5%)	5 (55,6%)	20 (64,5%)
I do not know what a virus or Trojan is	102 (22,7%)	87 (25,8%)	15 (13,4%)	6 (18,2%)	16 (17,6%)	34 (19,9%)	42 (31,3%)	4 (20%)	18 (28,6%)	13 (40,6%)	55 (22,3%)	15 (16%)	1 (7,7%)	12 (13,6%)	40 (25,6%)	3 (60%)	13 (39,4%)	25 (19,7%)	1 (11,1%)	8 (25,8%)
Is anti-virus currently installed on your computer?																				
Yes	270 (60,1%)	196 (58,2%)	74 (66,1%)	21 (63,6%)	49 (53,8%)	112 (65,5%)	72 (53,7%)	16 (80%)	36 (57,1%)	18 (56,3%)	151 (61,1%)	57 (60,6%)	8 (61,5%)	54 (61,4%)	87 (55,8%)	2 (40%)	17 (51,5%)	88 (69,3%)	7 (77,8%)	15 (48,4%)
No	51 (11,4%)	32 (9,5%)	19 (17%)	7 (21,2%)	9 (9,9%)	14 (8,2%)	20 (14,9%)	1 (5%)	2 (3,2%)	7 (21,9%)	28 (11,3%)	11 (11,7%)	3 (23,1%)	13 (14,8%)	15 (9,6%)	-	5 (15,2%)	10 (7,9%)	1 (11,1%)	7 (22,6%)
Do not know	128 (28,5%)	109 (32,3%)	19 (17%)	5 (15,2%)	33 (36,3%)	45 (26,3%)	42 (31,3%)	3 (15%)	25 (39,7%)	7 (21,9%)	68 (27,5%)	26 (27,7%)	2 (15,4%)	21 (23,9%)	54 (34,6%)	3 (60%)	11 (33,3%)	29 (22,8%)	1 (11,1%)	9 (29%)
How careful are you when you open an attachment in email?																				
I always make sure it is from a person I know	145 (32,3%)	101 (30%)	44 (39,3%)	11 (33,3%)	23 (25,3%)	53 (31%)	50 (37,3%)	8 (40%)	28 (44,4%)	8 (25%)	80 (32,4%)	27 (28,7%)	2 (15,4%)	24 (27,3%)	51 (32,7%)	1 (20%)	11 (33,3%)	43 (33,9%)	3 (33,3%)	12 (38,7%)

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.

and I am expecting the email																			
As long as I know the person or company that sent me the attachment, I open it	263 (58,6%)	204 (60,5%)	59 (52,7%)	21 (63,6%)	60 (65,9%)	104 (60,8%)	67 (50%)	11 (55%)	26 (41,3%)	15 (46,9%)	149 (60,3%)	64 (68,1%)	9 (69,2%)	60 (68,2%)	90 (57,7%)	3 (60%)	18 (54,5%)	72 (56,7%)	4 (44,4%)	16 (51,6%)
There is nothing wrong with opening attachments	41 (9,1%)	32 (9,5%)	9 (8%)	1 (3%)	8 (8,8%)	14 (8,2%)	17 (12,7%)	1 (5%)	9 (14,3%)	9 (28,1%)	18 (7,3%)	3 (3,2%)	2 (15,4%)	4 (4,5%)	15 (9,6%)	1 (20%)	4 (12,1%)	12 (9,4%)	2 (22,2%)	3 (9,7%)

Table 35: Non-ICT questionnaires - DYPE5 responses to viruses and trojans recognition, usage of anti-virus programs and handling of email attachments

Table 35 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- Have you ever found a virus or Trojan on your computer at work?
- Is anti-virus currently installed on your computer?
- How careful are you when you open an attachment in email?

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.

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
Do you know what a social-engineering attack is?																				
Yes	102 (22,7%)	66 (19,6%)	36 (32,1%)	3 (9,1%)	25 (27,5%)	41 (24,0%)	28 (20,9%)	5 (25%)	10 (15,9%)	10 (31,3%)	53 (21,5%)	23 (24,5%)	6 (46,2%)	23 (26,1%)	32 (20,5%)	-	8 (24,2%)	34 (26,8%)	2 (22,2%)	3 (9,7%)
No	347 (77,3%)	271 (80,4%)	76 (67,9%)	30 (90,9%)	66 (72,5%)	130 (76,0%)	106 (79,1%)	15 (75%)	53 (84,1%)	22 (68,8%)	194 (78,5%)	71 (75,5%)	7 (53,8%)	65 (73,9%)	124 (79,5%)	5 (100%)	25 (75,8%)	93 (73,2%)	7 (77,8%)	28 (90,3%)
Do you know what an email scam is and how to identify one?																				
Yes, I know what an email scam is and how to identify one	61 (13,6%)	32 (9,5%)	29 (25,9%)	6 (18,2%)	18 (19,8%)	24 (14,0%)	9 (6,7%)	4 (20%)	4 (6,3%)	3 (9,4%)	35 (14,2%)	14 (14,9%)	5 (38,5%)	21 (23,9%)	13 (8,3%)	-	6 (18,2%)	14 (11,0%)	4 (44,4%)	3 (9,7%)
I know what an email scam is, but I do not know how to identify one	114 (25,4%)	88 (26,1%)	26 (23,2%)	11 (33,3%)	23 (25,3%)	48 (28,1%)	28 (20,9%)	4 (20%)	11 (17,5%)	8 (25,0%)	65 (26,3%)	27 (28,7%)	3 (23,1%)	23 (26,1%)	37 (23,7%)	1 (20%)	9 (27,3%)	32 (25,2%)	1 (11,1%)	11 (35,5%)
No, I do not know what an email scam is or how to identify one	274 (61,0%)	217 (64,4%)	57 (50,9%)	16 (48,5%)	50 (54,9%)	99 (57,9%)	97 (72,4%)	12 (60%)	48 (76,2%)	21 (65,6%)	147 (59,5%)	53 (56,4%)	5 (38,5%)	44 (50,0%)	106 (67,9%)	4 (80%)	18 (54,5%)	81 (63,8%)	4 (44,4%)	17 (54,8%)
My computer has no value to hackers, they do not target me.																				
True	118 (26,3%)	87 (25,8%)	31 (27,7%)	5 (15,2%)	20 (22,0%)	46 (26,9%)	40 (29,9%)	7 (35%)	22 (34,9%)	8 (25,0%)	66 (26,7%)	20 (21,3%)	2 (15,4%)	19 (21,6%)	45 (28,8%)	2 (40%)	7 (21,2%)	32 (25,2%)	3 (33,3%)	10 (32,3%)

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.

False	331 (73,7%)	250 (74,2%)	81 (72,3%)	28 (84,8%)	71 (78,0%)	125 (73,1%)	94 (70,1%)	13 (65%)	41 (65,1%)	24 (75,0%)	181 (73,3%)	74 (78,7%)	11 (84,6%)	69 (78,4%)	111 (71,2%)	3 (60%)	26 (78,8%)	95 (74,8%)	6 (66,7%)	21 (67,7%)

Table 36: Non-ICT questionnaires - DYPE5 responses to social engineering attack acknowledge, email scam recognition and probability for being targeted from hackers

Table 36 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- Do you know what a social-engineering attack is?
- Do you know what an email scam is and how to identify one?
- My computer has no value to hackers, they do not target me.

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.

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?																				
Yes	94 (20,9%)	64 (19,0%)	30 (26,8%)	6 (18,2%)	19 (20,9%)	39 (22,8%)	26 (19,4%)	4 (20%)	10 (15,9%)	7 (21,9%)	44 (17,8%)	24 (25,5%)	9 (69,2%)	17 (19,3%)	24 (15,4%)	-	8 (24,2%)	36 (28,3%)	3 (33,3%)	6 (19,4%)
No	267 (59,5%)	206 (61,1%)	61 (54,5%)	17 (51,5%)	61 (67,0%)	104 (60,8%)	71 (53,0%)	14 (70%)	35 (55,6%)	20 (62,5%)	148 (59,9%)	61 (64,9%)	3 (23,1%)	47 (53,4%)	104 (66,7%)	4 (80%)	22 (66,7%)	68 (53,5%)	3 (33,3%)	19 (61,3%)
Do not know	88 (19,6%)	67 (19,9%)	21 (18,8%)	10 (30,3%)	11 (12,1%)	28 (16,4%)	37 (27,6%)	2 (10%)	18 (28,6%)	5 (15,6%)	55 (22,3%)	9 (9,6%)	1 (7,7%)	24 (27,3%)	28 (17,9%)	1 (20%)	3 (9,1%)	23 (18,1%)	3 (33,3%)	6 (19,4%)
Have you downloaded and installed software on your computer at work?																				
Yes	75 (16,7%)	48 (14,2%)	27 (24,1%)	6 (18,2%)	15 (16,5%)	36 (21,1%)	17 (12,7%)	1 (5%)	7 (11,1%)	4 (12,5%)	41 (16,6%)	18 (19,1%)	5 (38,5%)	24 (27,3%)	17 (10,9%)	1 (20%)	4 (12,1%)	26 (20,5%)	2 (22,2%)	1 (3,2%)
No	374 (83,3%)	289 (85,8%)	85 (75,9%)	27 (81,8%)	76 (83,5%)	135 (78,9%)	117 (87,3%)	19 (95%)	56 (88,9%)	28 (87,5%)	206 (83,4%)	76 (80,9%)	8 (61,5%)	64 (72,7%)	139 (89,1%)	4 (80%)	29 (87,9%)	101 (79,5%)	7 (77,8%)	30 (96,8%)
Have you given your password to your colleagues or your manager, when you were asked for it?																				
Yes	146 (32,5%)	116 (34,4%)	30 (26,8%)	13 (39,4%)	32 (35,2%)	56 (32,7%)	42 (31,3%)	3 (15%)	22 (34,9%)	6 (18,8%)	81 (32,8%)	34 (36,2%)	3 (23,1%)	18 (20,5%)	44 (28,2%)	1 (20%)	6 (18,2%)	60 (47,2%)	2 (22,2%)	15 (48,4%)
No	303 (67,5%)	221 (65,6%)	82 (73,2%)	20 (60,6%)	59 (64,8%)	115 (67,3%)	92 (68,7%)	17 (85%)	41 (65,1%)	26 (81,3%)	166 (67,2%)	60 (63,8%)	10 (76,9%)	70 (79,5%)	112 (71,8%)	4 (80%)	27 (81,8%)	67 (52,8%)	7 (77,8%)	16 (51,6%)

Table 37: Non-ICT questionnaires - DYPE5 responses to personal devices usage policies, employees' administrative rights on computers and password sharing

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 37 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?
- Have you downloaded and installed software on your computer at work?
- Have you given your password to your colleagues or your manager, when you were asked for it?

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.

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
Which of these is closer to your thinking, even if neither is exactly right?																				
Following security policies at our hospital prevents me from doing my job	50 (11,1%)	27 (8%)	23 (20,5%)	10 (30,3%)	8 (8,8%)	17 (9,9%)	14 (10,4%)	1 (5%)	5 (7,9%)	2 (6,3%)	31 (12,6%)	10 (10,6%)	2 (15,4%)	18 (20,5%)	15 (9,6%)	-	2 (6,1%)	13 (10,2%)	-	2 (6,5%)
Following security policies at our hospital helps me do my job better	399 (88,9%)	310 (92%)	89 (79,5%)	23 (69,7%)	83 (91,2%)	154 (90,1%)	120 (89,6%)	19 (95%)	58 (92,1%)	30 (93,8%)	216 (87,4%)	84 (89,4%)	11 (84,6%)	70 (79,5%)	141 (90,4%)	5 (100%)	31 (93,9%)	114 (89,8%)	9 (100%)	29 (93,5%)
I feel I have been sufficiently trained in security at our hospital.																				
Strongly agree	5 (1,1%)	4 (1,2%)	1 (0,9%)	-	1 (1,1%)	2 (1,2%)	1 (0,7%)	3 (15%)	1 (1,6%)	1 (3,1%)	2 (0,8%)	1 (1,1%)	-	-	-	-	4 (12,1%)	1 (0,8%)	-	-
Agree	41 (9,1%)	28 (8,3%)	13 (11,6%)	3 (9,1%)	3 (3,3%)	19 (11,1%)	13 (9,7%)	8 (40%)	7 (11,1%)	6 (18,8%)	23 (9,3%)	5 (5,3%)	-	3 (3,4%)	13 (8,3%)	-	5 (15,2%)	16 (12,6%)	1 (11,1%)	3 (9,7%)
Neither agree nor disagree	120 (26,7%)	91 (27%)	29 (25,9%)	6 (18,2%)	34 (37,4%)	34 (19,9%)	41 (30,6%)	5 (25%)	20 (31,7%)	11 (34,4%)	59 (23,9%)	27 (28,7%)	3 (23,1%)	21 (23,9%)	38 (24,4%)	2 (40%)	7 (21,2%)	42 (33,1%)	2 (22,2%)	8 (25,8%)
Disagree	179 (39,9%)	135 (40,1%)	44 (39,3%)	16 (48,5%)	32 (35,2%)	75 (43,9%)	48 (35,8%)	3 (15%)	23 (36,5%)	9 (28,1%)	103 (41,7%)	38 (40,4%)	6 (46,2%)	39 (44,3%)	62 (39,7%)	2 (40%)	11 (33,3%)	44 (34,6%)	5 (55,6%)	16 (51,6%)
Strongly disagree	104 (23,2%)	79 (23,4%)	25 (22,3%)	8 (24,2%)	21 (23,1%)	41 (24%)	31 (23,1%)	1 (5%)	12 (19%)	5 (15,6%)	60 (24,3%)	23 (24,5%)	4 (30,8%)	25 (28,4%)	43 (27,6%)	1 (20%)	6 (18,2%)	24 (18,9%)	1 (11,1%)	4 (12,9%)

Table 38: Non-ICT questionnaires - DYPE5 responses to thoughts about following security policies and security training

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 38 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- Following security policies at our hospital prevents me from doing my job OR Following security policies at our hospital helps me do my job better
- I feel I have been sufficiently trained in security at our 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.

	Total	Gender		Age					Education					Position						
	n = 449 (100%)	Female (n = 337)	Male (n = 112)	21-30 (n = 33)	31-40 (n = 91)	41-50 (n = 171)	51-60 (n = 134)	>61 (n = 20)	Secondary Education (n = 63)	Vocational training institute (n = 32)	Bachelor Degree (n = 247)	MSc (n = 94)	PhD (n = 13)	Doctor (n = 88)	Nurse (n = 156)	Auxiliary personnel (n = 5)	Lab. Personnel (n = 33)	Administrative personnel (n = 127)	Technical personnel (n = 9)	Other (n = 31)
I am confident that I could recognize a security issue or incident if I saw one.																				
Strongly agree	18 (4%)	8 (2,4%)	10 (8,9%)	1 (3%)	2 (2,2%)	6 (3,5%)	8 (6%)	1 (5%)	2 (3,2%)	1 (3,1%)	9 (3,6%)	5 (5,3%)	1 (7,7%)	2 (2,3%)	5 (3,2%)	-	2 (6,1%)	9 (7,1%)	-	-
Agree	107 (23,8%)	70 (20,8%)	37 (33,0%)	14 (42,4%)	26 (28,6%)	39 (22,8%)	23 (17,2%)	5 (25%)	13 (20,6%)	9 (28,1%)	57 (23,1%)	26 (27,7%)	2 (15,4%)	21 (23,9%)	36 (23,1%)	-	10 (30,3%)	28 (22,1%)	2 (22,2%)	10 (32,3%)
Neither agree nor disagree	191 (42,5%)	151 (44,8%)	40 (35,7%)	12 (36,4%)	41 (45,1%)	78 (45,6%)	53 (39,6%)	7 (35%)	25 (39,7%)	13 (40,6%)	113 (45,7%)	34 (36,2%)	6 (46,2%)	40 (45,5%)	63 (40,4%)	4 (80%)	9 (27,3%)	58 (45,7%)	3 (33,3%)	14 (45,2%)
Disagree	102 (22,7%)	79 (23,4%)	23 (20,5%)	5 (15,2%)	18 (19,8%)	37 (21,6%)	35 (26,1%)	7 (35%)	17 (27%)	7 (21,9%)	52 (21,1%)	22 (23,4%)	4 (30,8%)	21 (23,9%)	38 (24,4%)	-	9 (27,3%)	25 (19,7%)	4 (44,4%)	5 (16,1%)
Strongly disagree	31 (6,9%)	29 (8,6%)	2 (1,,8%)	1 (3%)	4 (4,4%)	11 (6,4%)	15 (11,2%)	-	6 (9,5%)	2 (6,3%)	16 (6,5%)	7 (7,4%)	-	4 (4,6%)	14 (9%)	1 (20%)	3 (9,1%)	7 (5,5%)	-	2 (6,5%)
Do you lock your PC when you leave your office even for a while?																				
Yes	219 (48,8%)	158 (46,9%)	61 (54,5%)	19 (57,6%)	47 (51,6%)	80 (46,8%)	62 (46,3%)	11 (55%)	27 (42,9%)	18 (56,3%)	119 (48,2%)	49 (52,1%)	6 (46,2%)	49 (55,7%)	80 (51,3%)	2 (40%)	14 (42,4%)	54 (42,5%)	5 (55,6%)	15 (48,4%)
No	230 (51,2%)	179 (53,1%)	51 (45,5%)	14 (42,4%)	44 (48,4%)	91 (53,2%)	72 (53,7%)	9 (45%)	36 (57,1%)	14 (43,8%)	128 (51,8%)	45 (47,9%)	7 (53,8%)	39 (44,3%)	76 (48,7%)	3 (60%)	19 (57,6%)	73 (57,5%)	4 (44,4%)	16 (51,6%)

Table 39: Non-ICT questionnaires - DYPE5 responses to security issue recognition and PC locking when away from office

Table 39 contains DYPE5 non-ICT personnel responses to the following sentences/questions:

- I am confident that I could recognize a security issue or incident if I saw one
- Do you lock your PC when you leave your office even for a while?

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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute (n=10)	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
Does your hospital have a Cyber-Security Department or external services?																				
Yes	41 (32,5%)	33 (31,4%)	8 (38,1%)	7 (36,8%)	12 (42,9%)	19 (28,8%)	2 (20%)	1 (33,3%)	3 (33,3%)	6 (60%)	15 (22,1%)	13 (44,8%)	4 (40%)	9 (24,3%)	19 (33,3%)	-	-	8 (34,8%)	2 (100%)	3 (100%)
No	33 (26,2%)	26 (24,8%)	7 (33,3%)	3 (15,8%)	3 (10,7%)	22 (33,3%)	4 (40%)	1 (33,3%)	2 (22,2%)	1 (10%)	19 (27,9%)	6 (20,7%)	5 (50%)	11 (29,7%)	11 (19,3%)	-	2 (66,7%)	9 (39,1%)	-	-
Do not know	52 (41,3%)	46 (43,8%)	6 (28,6%)	9 (47,4%)	13 (46,4%)	25 (37,9%)	4 (40%)	1 (33,3%)	4 (44,4%)	3 (30%)	34 (50%)	10 (34,5%)	1 (10%)	17 (45,9%)	27 (47,4%)	1 (100%)	1 (33,3%)	6 (26,1%)	-	-
Does your work on the hospital involves working on a computer at any time?																				
Yes	123 (97,6%)	103 (98,1%)	20 (95,2%)	19 (100%)	28 (100%)	63 (95,5%)	10 (100%)	3 (100%)	8 (88,9%)	10 (100%)	67 (98,5%)	29 (100%)	9 (90%)	36 (97,3%)	55 (96,5%)	1 (100%)	3 (100%)	23 (100%)	2 (100%)	3 (100%)
No	3 (2,4%)	2 (1,9%)	1 (4,8%)	-	-	3 (4,5%)	-	-	1 (11,1%)	-	1 (1,5%)	-	1 (10%)	1 (2,7%)	2 (3,5%)	-	-	-	-	-
Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?																				
Yes	107 (84,9%)	93 (88,6%)	14 (66,7%)	19 (100%)	24 (85,7%)	52 (78,8%)	10 (100%)	2 (66,7%)	9 (100%)	10 (100%)	58 (85,3%)	23 (79,3%)	7 (70%)	28 (75,7%)	49 (86%)	1 (100%)	2 (66,7%)	22 (95,7%)	2 (100%)	3 (100%)
No	19 (15,1%)	12 (11,4%)	7 (33,3%)	-	4 (14,3%)	14 (21,2%)	-	1 (33,3%)	-	-	10 (14,7%)	6 (20,7%)	3 (30%)	9 (24,3%)	8 (14%)	-	1 (33,3%)	1 (4,3%)	-	-

Table 40: Non-ICT questionnaires - Polaris responses to cyber security support services existence, number of computer related job positions and GDPR training

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 40 contains Polaris non-ICT personnel responses to the following sentences/questions:

- Does your hospital have a Cyber-Security Department or external services?
- Does your work on the hospital involves working on a computer at any time?
- Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?

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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute (n=10)	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
Does your work in the hospital involves access to patient data, which is considered confidential and sensitive information?																				
Yes	117 (92,9%)	97 (92,4%)	20 (95,2%)	17 (89,5%)	27 (96,4%)	60 (90,9%)	10 (100%)	3 (100%)	9 (100%)	8 (80%)	62 (91,2%)	28 (96,6%)	10 (100%)	34 (91,9%)	52 (91,2%)	1 (100%)	3 (100%)	22 (95,7%)	2 (100%)	3 (100%)
No	9 (7,1%)	8 (7,6%)	1 (4,8%)	2 (10,5%)	1 (3,6%)	6 (9,1%)	-	-	-	2 (20%)	6 (8,8%)	1 (3,4%)	-	3 (8,1%)	5 (8,8%)	-	-	1 (4,3%)	-	-
Do you have cyber-security policies at your hospital?																				
Yes	75 (59,5%)	59 (56,2%)	16 (76,2%)	11 (57,9%)	20 (71,4%)	36 (54,5%)	6 (60%)	2 (66,7%)	8 (88,9%)	7 (70%)	33 (48,5%)	22 (75,9%)	5 (50%)	21 (56,8%)	31 (54,4%)	1 (100%)	1 (33,3%)	16 (69,6%)	2 (100%)	3 (100%)
No	9 (7,1%)	8 (7,6%)	1 (4,8%)	-	-	7 (10,6%)	2 (20%)	-	-	-	8 (11,8%)	1 (3,4%)	-	4 (10,8%)	5 (8,8%)	-	-	-	-	-
Do not know	42 (33,3%)	38 (36,2%)	4 (19%)	8 (42,1%)	8 (28,6%)	23 (34,8%)	2 (20%)	1 (33,3%)	1 (11,1%)	3 (30%)	27 (39,7%)	6 (20,7%)	5 (50%)	12 (32,4%)	21 (36,8%)	-	2 (66,7%)	7 (30,4%)	-	-

Table 41: Non-ICT questionnaires - Polaris responses to patient data access and cyber security policies existence

Table 41 contains Polaris non-ICT personnel responses to the following sentences/questions:

- Does your work in the hospital involves access to patient data, which is considered confidential and sensitive information?
- Do you have cyber-security policies at your 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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
Do you know when your computer is hacked or infected, and whom to contact when it occurs?																				
Yes, I know when my computer is hacked or infected and I know whom to contact	78 (61,9%)	64 (61%)	14 (66,7%)	10 (52,6%)	19 (67,9%)	39 (59,1%)	8 (80%)	2 (66,7%)	8 (88,9%)	7 (70%)	41 (60,3%)	18 (62,1%)	4 (40%)	22 (59,5%)	36 (63,2%)	-	1 (33,3%)	15 (65,2%)	2 (100%)	2 (66,7%)
No, I do not know when my computer is hacked or infected and I don't know whom to contact.	9 (7,1%)	8 (7,6%)	1 (4,8%)	-	2 (7,1%)	6 (9,1%)	-	-	1 (11,1%)	1 (10%)	5 (7,4%)	2 (6,9%)	-	2 (5,4%)	7 (12,3%)	-	-	-	-	-
Yes, I know when my computer is hacked or infected but I don't know whom to contact	3 (2,4%)	2 (1,9%)	1 (4,8%)	1 (5,3%)	1 (3,6%)	2 (3%)	-	-	-	-	3 (4,4%)	-	-	2 (5,4%)	1 (1,8%)	-	-	-	-	-
No, I do not know when my computer and I know whom to contact	36 (28,6%)	31 (29,5%)	5 (23,8%)	8 (42,1%)	6 (21,4%)	19 (28,8%)	2 (20%)	1 (33,3%)	-	2 (20%)	19 (27,9%)	9 (31%)	6 (60%)	11 (29,7%)	13 (22,8%)	1 (100%)	2 (66,7%)	8 (34,8%)	-	1 (33,3%)

Table 42: Non-ICT questionnaires - Polaris responses to acknowledge of hacked or infected computer

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 42 contains Polaris non-ICT personnel responses to the following sentences/questions:

- Do you know when your computer is hacked or infected, and whom to contact when it occurs?

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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute (n=10)	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
Have you ever found a virus or Trojan on your computer at work?																				
Yes, my computer has been infected before	27 (21,4%)	20 (19%)	7 (33,3%)	1 (5,3%)	5 (17,9%)	19 (28,8%)	2 (20%)	-	9 (100%)	2 (20%)	13 (19,1%)	8 (27,6%)	4 (40%)	11 (29,7%)	10 (17,5%)	-	-	4 (17,4%)	1 (50%)	-
No, my computer has never been infected	85 (67,5%)	73 (69,5%)	12 (57,1%)	15 (78,9%)	19 (67,9%)	41 (62,1%)	7 (70%)	3 (100%)	-	7 (70%)	42 (61,8%)	21 (72,4%)	6 (60%)	21 (56,8%)	38 (66,7%)	1 (100%)	-	19 (82,6%)	1 (50%)	3 (100%)
I do not know what a virus or Trojan is	14 (11,1%)	12 (11,4%)	2 (9,5%)	3 (15,8%)	4 (14,3%)	6 (9,1%)	1 (10%)	-	-	1 (10%)	13 (19,1%)	-	-	5 (13,5%)	9 (15,8%)	-	-	-	-	-
Is anti-virus currently installed on your computer?																				
Yes	99 (78,6%)	85 (81%)	14 (66,7%)	15 (78,9%)	22 (78,6%)	52 (78,8%)	8 (80%)	2 (66,7%)	7 (77,8%)	8 (80%)	49 (72,1%)	27 (93,1%)	8 (80%)	27 (73%)	41 (71,9%)	1 (100%)	2 (66,7%)	23 (100%)	2 (100%)	2 (66,7%)
No	6 (4,8%)	4 (3,8%)	2 (9,5%)	-	-	4 (6,1%)	1 (10%)	1 (33,3%)	2 (22,2%)	1 (10%)	3 (4,4%)	-	-	1 (2,7%)	5 (8,8%)	-	-	-	-	-
Do not know	21 (16,7%)	16 (15,2%)	5 (23,8%)	4 (21,1%)	6 (21,4%)	10 (15,2%)	1 (10%)	-	-	1 (10%)	16 (23,5%)	2 (6,9%)	2 (20%)	9 (24,3%)	11 (19,3%)	-	-	-	-	1 (33,3%)
How careful are you when you open an attachment in email?																				
I always make sure it is from a person I know and I am expecting the email	63 (50%)	54 (51,4%)	9 (42,9%)	9 (47,4%)	13 (46,4%)	37 (56,1%)	3 (30%)	1 (33,3%)	3 (33,3%)	4 (40%)	35 (51,5%)	15 (51,7%)	6 (60%)	16 (43,2%)	29 (50,9%)	-	1 (33,3%)	13 (56,5%)	2 (100%)	2 (66,7%)

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.

As long as I know the person or company that sent me the attachment, I open it	57 (45,2%)	47 (44,8%)	10 (47,6%)	10 (52,6%)	14 (50%)	26 (39,4%)	6 (60%)	1 (33,3%)	6 (66,7%)	6 (60%)	29 (42,6%)	12 (41,4%)	4 (40%)	19 (51,4%)	24 (42,1%)	1 (100%)	2 (66,7%)	10 (43,5%)	-	1 (33,3%)
There is nothing wrong with opening attachments	6 (4,8%)	4 (3,8%)	2 (9,5%)	-	1 (3,6%)	3 (4,5%)	1 (10%)	1 (33,3%)	-	-	4 (5,9%)	2 (6,9%)	-	2 (5,4%)	4 (7%)	-	-	-	-	-

Table 43: Non-ICT questionnaires - Polaris responses to viruses and trojans recognition, usage of anti-virus programs and handling of email attachments

Table 43 contains Polaris non-ICT personnel responses to the following sentences/questions:

- Have you ever found a virus or Trojan on your computer at work?
- Is anti-virus currently installed on your computer?
- How careful are you when you open an attachment in email?

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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
Do you know what a social-engineering attack is?																				
Yes	40 (31,7%)	31 (29,5%)	9 (42,9%)	5 (26,3%)	4 (14,3%)	27 (40,9%)	2 (20%)	2 (66,7%)	4 (44,4%)	3 (30%)	21 (30,9%)	10 (34,5%)	2 (20%)	8 (21,6%)	21 (36,8%)	-	1 (33,3%)	9 (39,1%)	1 (50%)	-
No	86 (68,3%)	74 (70,5%)	12 (57,1%)	14 (73,7%)	24 (85,7%)	39 (59,1%)	8 (80%)	1 (33,3%)	5 (55,6%)	7 (70%)	47 (69,1%)	19 (65,5%)	8 (80%)	29 (78,4%)	36 (63,2%)	1 (100%)	2 (66,7%)	14 (60,9%)	1 (50%)	3 (100%)
Do you know what an email scam is and how to identify one?																				
Yes, I know what an email scam is and how to identify one	47 (37,3%)	34 (32,4%)	13 (61,9%)	8 (42,1%)	9 (32,1%)	29 (43,9%)	1 (10%)	-	4 (44,4%)	5 (50%)	21 (30,9%)	13 (44,8%)	4 (40%)	14 (37,8%)	19 (33,3%)	1 (100%)	2 (66,7%)	9 (39,1%)	2 (100%)	-
I know what an email scam is, but I do not know how to identify one	41 (32,5%)	35 (33,3%)	6 (28,6%)	7 (36,8%)	8 (28,6%)	20 (30,3%)	3 (30%)	3 (100%)	2 (22,2%)	3 (30%)	22 (32,4%)	11 (37,9%)	3 (30%)	11 (29,7%)	18 (31,6%)	-	1 (33,3%)	10 (43,5%)	-	1 (33,3%)
No, I do not know what an email scam is or how to identify one	38 (30,2%)	36 (34,3%)	2 (9,5%)	4 (21,1%)	11 (39,3%)	17 (25,8%)	6 (60%)	-	3 (33,3%)	2 (20%)	25 (36,8%)	5 (17,2%)	3 (30%)	12 (32,4%)	20 (35,1%)	-	-	4 (17,4%)	-	2 (66,7%)
My computer has no value to hackers, they do not target me.																				
True	16 (12,7%)	14 (13,3%)	2 (9,5%)	3 (15,8%)	2 (7,1%)	11 (16,7%)	-	-	-	3 (30%)	6 (8,8%)	6 (20,7%)	1 (10%)	-	7 (12,3%)	-	-	4 (17,4%)	-	1 (33,3%)
False	110 (87,3%)	91 (86,7%)	19 (90,5%)	16 (84,2%)	26 (92,9%)	55 (83,3%)	10 (100%)	3 (100%)	9 (100%)	7 (70%)	62 (91,2%)	23 (79,3%)	9 (90%)	-	50 (87,7%)	1 (100%)	3 (100%)	19 (82,6%)	2 (100%)	2 (66,7%)

Table 44: Non-ICT questionnaires - Polaris responses to social engineering attack acknowledge, email scam recognition and probability for being targeted from hackers

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 44 contains Polaris non-ICT personnel responses to the following sentences/questions:

- Do you know what a social-engineering attack is?
- Do you know what an email scam is and how to identify one?
- My computer has no value to hackers, they do not target me.

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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute (n=10)	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?																				
Yes	30 (23,8%)	20 (19%)	10 (47,6%)	2 (10,5%)	10 (35,7%)	17 (25,8%)	1 (10%)	-	1 (11,1%)	1 (10%)	20 (29,4%)	5 (17,2%)	3 (30%)	11 (29,7%)	9 (15,8%)	1 (100%)	1 (33,3%)	5 (21,7%)	2 (100%)	1 (33,3%)
No	79 (62,7%)	69 (65,7%)	10 (47,6%)	13 (68,4%)	13 (46,4%)	43 (65,2%)	7 (70%)	3 (100%)	7 (77,8%)	8 (80%)	34 (50%)	24 (82,8%)	6 (60%)	21 (56,8%)	37 (64,9%)	-	2 (66,7%)	18 (78,3%)	-	1 (33,3%)
Do not know	17 (13,5%)	16 (15,2%)	1 (4,8%)	4 (21,1%)	5 (17,9%)	6 (9,1%)	2 (20%)	-	1 (11,1%)	1 (10%)	14 (20,6%)	-	1 (10%)	5 (13,5%)	11 (19,3%)	-	-	-	-	1 (33,3%)
Have you downloaded and installed software on your computer at work?																				
Yes	21 (16,7%)	15 (14,3%)	6 (28,6%)	1 (5,3%)	6 (21,4%)	14 (21,2%)	-	-	-	1 (10%)	14 (20,6%)	3 (10,3%)	3 (30%)	8 (21,6%)	4 (7%)	-	1 (33,3%)	5 (21,7%)	2 (100%)	1 (33,3%)
No	105 (83,3%)	90 (85,7%)	15 (71,4%)	18 (94,7%)	22 (78,6%)	52 (78,8%)	10 (100%)	3 (100%)	9 (100%)	9 (90%)	54 (79,4%)	26 (89,7%)	7 (70%)	29 (78,4%)	53 (93%)	1 (100%)	2 (66,7%)	18 (78,3%)	-	2 (66,7%)
Have you given your password to your colleagues or your manager, when you were asked for it?																				
Yes	38 (30,2%)	35 (33,3%)	3 (14,3%)	8 (42,1%)	11 (39,3%)	18 (27,3%)	1 (10%)	-	-	5 (50%)	23 (33,8%)	9 (31%)	1 (10%)	11 (29,7%)	15 (26,3%)	1 (100%)	-	9 (39,1%)	-	2 (66,7%)
No	88 (69,8%)	70 (66,7%)	18 (85,7%)	11 (57,9%)	17 (60,7%)	48 (72,7%)	9 (90%)	3 (100%)	9 (100%)	5 (50%)	45 (66,2%)	20 (69%)	9 (90%)	26 (70,3%)	42 (73,7%)	-	3 (100%)	14 (60,9%)	2 (100%)	1 (33,3%)

Table 45: Non-ICT questionnaires - Polaris responses to personal devices usage policies, employees' administrative rights on computers and password sharing

Table 45 contains Polaris non-ICT personnel responses to the following sentences/questions:

- Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?

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.

- Have you downloaded and installed software on your computer at work?
- Have you given your password to your colleagues or your manager, when you were asked for it?

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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute (n=10)	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
Which of these is closer to your thinking, even if neither is exactly right?																				
Following security policies at our hospital prevents me from doing my job	17 (13,5%)	14 (13,3%)	3 (14,3%)	3 (15,8%)	2 (7,1%)	11 (16,7%)	-	1 (33,3%)	-	2 (20%)	8 (11,8%)	5 (17,2%)	2 (20%)	8 (21,6%)	7 (12,3%)	-	-	-	-	2 (66,7%)
Following security policies at our hospital helps me do my job better	109 (86,5%)	91 (86,7%)	18 (85,7%)	16 (84,2%)	26 (92,9%)	55 (83,3%)	10 (100%)	2 (66,7%)	9 (100%)	8 (80%)	60 (88,2%)	24 (82,8%)	8 (80%)	29 (78,4%)	50 (87,7%)	1 (100%)	3 (100%)	23 (100%)	2 (100%)	1 (33,3%)
I feel I have been sufficiently trained in security at our hospital.																				
Strongly agree	23 (18,3%)	19 (18,1%)	4 (19%)	4 (21,1%)	3 (10,7%)	14 (21,2%)	1 (10%)	1 (33,3%)	2 (22,2%)	4 (40%)	11 (16,2%)	6 (20,7%)	-	2 (5,4%)	13 (22,8%)	-	1 (33,3%)	6 (26,1%)	1 (50%)	-
Agree	65 (51,6%)	56 (53,3%)	9 (42,9%)	14 (73,7%)	15 (53,6%)	28 (42,4%)	7 (70%)	1 (33,3%)	7 (77,8%)	5 (50%)	32 (47,1%)	16 (55,2%)	5 (50%)	17 (45,9%)	28 (49,1%)	1 (100%)	1 (33,3%)	15 (65,2%)	1 (50%)	2 (66,7%)
Neither agree nor disagree	15 (11,9%)	14 (13,3%)	1 (4,8%)	1 (5,3%)	3 (10,7%)	9 (13,6%)	1 (10%)	1 (33,3%)	-	1 (10%)	12 (17,6%)	1 (3,4%)	2 (20%)	8 (21,6%)	6 (10,5%)	-	-	-	-	1 (33,3%)
Disagree	7 (5,6%)	5 (4,8%)	2 (9,5%)	-	2 (7,1%)	5 (7,6%)	1 (10%)	-	-	-	4 (5,9%)	2 (6,9%)	1 (10%)	7 (18,9%)	6 (10,5%)	-	1 (33,3%)	2 (8,7%)	-	-
Strongly disagree	16 (12,7%)	11 (10,5%)	5 (23,8%)	-	5 (17,9%)	10 (15,2%)	-	-	-	-	9 (13,2%)	4 (13,8%)	2 (20%)	3 (8,1%)	4 (7%)	-	-	-	-	-

Table 46: Non-ICT questionnaires - Polaris responses to thoughts about following security policies and security training

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 46 contains Polaris non-ICT personnel responses to the following sentences/questions:

- Following security policies at our hospital prevents me from doing my job OR Following security policies at our hospital helps me do my job better
- I feel I have been sufficiently trained in security at our 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.

	Total	Gender		Age					Education					Position						
	n = 126 (100%)	Female (n=105)	Male(n=21)	21-30 (n=19)	31-40 (n=28)	41-50 (n=66)	51-60 (n=10)	>61 (n=3)	Secondary Education (n=9)	Vocational training institute (n=10)	Bachelor Degree (n=68)	MSc (n=29)	PhD (n=10)	Doctor(n=37)	Nurse (n=57)	Auxiliary personnel(n=1)	Lab. personnel (n=3)	Administrative personnel (n=23)	Technical personnel (n=2)	Other (n=3)
I am confident that I could recognize a security issue or incident if I saw one.																				
Strongly agree	17 (13,5%)	11 (10,5%)	6 (28,6%)	2 (10,5%)	1 (3,6%)	12 (18,2%)	1 (10%)	1 (33,3%)	1 (11,1%)	3 (30%)	8 (11,8%)	4 (13,8%)	1 (10%)	3 (8,1%)	8 (14%)	-	1 (33,3%)	4 (17,4%)	1 (50%)	-
Agree	74 (58,7%)	63 (60%)	11 (52,4%)	14 (73,7%)	18 (64,3%)	34 (51,5%)	7 (70%)	1 (33,3%)	8 (88,9%)	5 (50%)	36 (52,9%)	19 (65,5%)	6 (60%)	20 (54,1%)	34 (59,6%)	1 (100%)	1 (33,3%)	15 (65,2%)	1 (50%)	2 (66,7%)
Neither agree nor disagree	10 (7,9%)	9 (8,6%)	1 (4,8%)	2 (10,5%)	2 (7,1%)	5 (7,6%)	1 (10%)	-	-	-	8 (11,8%)	2 (6,9%)	-	6 (16,2%)	3 (5,3%)	-	-	-	-	1 (33,3%)
Disagree	22 (17,5%)	20 (19%)	2 (9,5%)	1 (5,3%)	6 (21,4%)	13 (19,7%)	1 (10%)	1 (33,3%)	-	2 (20%)	13 (19,1%)	4 (13,8%)	3 (30%)	8 (21,6%)	9 (15,8%)	-	1 (33,3%)	4 (17,4%)	-	-
Strongly disagree	3 (2,4%)	2 (1,9%)	1 (4,8%)	-	1 (3,6%)	2 (3%)	-	-	-	-	3 (4,4%)	-	-	-	3 (5,3%)	-	-	-	-	-
Do you lock your PC when you leave your office even for a while?																				
Yes	56 (44,4%)	43 (41%)	13 (61,9%)	7 (36,8%)	13 (46,4%)	30 (45,5%)	5 (50%)	1 (33,3%)	5 (55,6%)	3 (30%)	27 (39,7%)	16 (55,2%)	5 (50%)	14 (37,8%)	24 (42,1%)	1 (100%)	1 (33,3%)	13 (56,5%)	2 (100%)	1 (33,3%)
No	70 (55,6%)	62 (59%)	8 (38,1%)	12 (63,2%)	15 (53,6%)	36 (54,5%)	5 (50%)	2 (66,7%)	4 (44,4%)	7 (70%)	41 (60,3%)	13 (44,8%)	5 (50%)	23 (62,2%)	33 (57,9%)	-	2 (66,7%)	10 (43,5%)	-	2 (66,7%)

Table 47: Non-ICT questionnaires - Polaris responses to security issue recognition and PC locking when away from office

Table 47 contains Polaris non-ICT personnel responses to the following sentences/questions:

- I am confident that I could recognize a security issue or incident if I saw one
- Do you lock your PC when you leave your office even for a while?

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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training institute (n=10)	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
Does your hospital have a Cyber-Security Department or external services?																				
Yes	46 (37,1%)	30 (38,5%)	16 (34,8%)	2 (20%)	9 (25%)	20 (44,4%)	9 (45%)	6 (46,2%)	15 (35,7%)	1 (10%)	2 (40%)	28 (42,4%)	-	9 (40,9%)	8 (47,1%)	2 (16,7%)	3 (42,9%)	20 (39,2%)	2 (28,6%)	2 (25%)
No	78 (62,9%)	48 (61,5%)	30 (65,2%)	8 (80%)	27 (75%)	25 (55,6%)	11 (55%)	7 (53,8%)	27 (64,3%)	9 (90%)	3 (60%)	38 (57,6%)	1 (100%)	13 (59,1%)	9 (52,9%)	10 (83,3%)	4 (57,1%)	31 (60,8%)	5 (71,4%)	6 (75%)
Do not know	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Does your work on the hospital involves working on a computer at any time?																				
Yes	121 (97,6%)	76 (97,4%)	45 (97,8%)	9 (90%)	36 (100%)	44 (97,8%)	19 (95%)	13 (100%)	39 (92,9%)	10 (100%)	5 (100%)	66 (100%)	1 (100%)	22 (100%)	17 (100%)	11 (91,7%)	7 (100%)	49 (96,1%)	7 (100%)	8 (100%)
No	3 (2,4%)	2 (2,6%)	1 (2,2%)	1 (10%)	-	1 (2,2%)	1 (5%)	-	3 (7,1%)	-	-	-	-	-	-	1 (8,3%)	-	2 (3,9%)	-	-
Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?																				
Yes	63 (50,8%)	42 (53,8%)	21 (45,7%)	2 (20%)	18 (50%)	24 (53,3%)	13 (65%)	6 (46,2%)	20 (47,6%)	6 (60%)	2 (40%)	34 (51,5%)	1 (100%)	13 (59,1%)	9 (52,9%)	2 (16,7%)	5 (71,4%)	28 (54,9%)	5 (71,4%)	4 (50%)
No	61 (49,2%)	36 (46,2%)	25 (54,3%)	8 (80%)	18 (50%)	21 (46,7%)	7 (35%)	7 (53,8%)	22 (52,4%)	4 (40%)	3 (60%)	32 (48,5%)	-	9 (40,9%)	8 (47,1%)	10 (83,3%)	2 (28,6%)	23 (45,1%)	2 (28,6%)	4 (50%)

Table 48: Non-ICT questionnaires - HESE responses to cyber security support services existence, number of computer related job positions and GDPR training

Table 48 contains HESE non-ICT personnel responses to the following sentences/questions:

- Does your hospital have a Cyber-Security Department or external services?
- Does your work on the hospital involves working on a computer at any time?
- Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?

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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training institute (n=10)	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
Does your work in the hospital involves access to patient data, which is considered confidential and sensitive information?																				
Yes	89 (71,8%)	61 (78,2%)	28 (60,9%)	4 (40%)	28 (77,8%)	33 (73,3%)	16 (80%)	8 (61,5%)	24 (57,1%)	5 (50%)	3 (60%)	57 (86,4%)	-	22 (100%)	16 (94,1%)	3 (25%)	7 (100%)	35 (68,6%)	2 (28,6%)	4 (50%)
No	35 (28,2%)	17 (21,8%)	18 (39,1%)	6 (60%)	8 (22,2%)	12 (26,7%)	4 (20%)	5 (38,5%)	18 (42,9%)	5 (50%)	2 (40%)	9 (13,6%)	1 (100%)	-	1 (5,9%)	9 (75%)	-	16 (31,4%)	5 (71,4%)	4 (50%)
Do you have cyber-security policies at your hospital?																				
Yes	68 (54,8%)	42 (53,9%)	26 (56,5%)	7 (70%)	16 (44,4%)	28 (62,2%)	11 (55%)	6 (46,2%)	21 (50%)	4 (40%)	4 (80%)	38 (57,6%)	1 (100%)	11 (50%)	11 (64,7%)	6 (50%)	5 (71,4%)	26 (51%)	3 (42,9%)	6 (75%)
No	3 (2,4%)	3 (3,8%)	-	-	3 (8,3%)	-	-	-	1 (2,4%)	-	-	2 (3%)	-	-	-	-	1 (14,3%)	2 (3,9%)	-	-
Do not know	53 (42,7%)	33 (42,3%)	20 (43,5%)	3 (30%)	17 (47,2%)	17 (37,8%)	9 (45%)	7 (53,8%)	20 (47,6%)	6 (60%)	1 (20%)	26 (39,4%)	-	11 (50%)	6 (35,3%)	6 (50%)	1 (14,3%)	23 (45,1%)	4 (57,1%)	2 (25%)

Table 49: Non-ICT questionnaires - HESE responses to patient data access and cyber security policies existence

Table 49 contains HESE non-ICT personnel responses to the following sentences/questions:

- Does your work in the hospital involves access to patient data, which is considered confidential and sensitive information?
- Do you have cyber-security policies at your 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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
Do you know when your computer is hacked or infected, and whom to contact when it occurs?																				
Yes, I know when my computer is hacked or infected and I know whom to contact.	65 (52,4%)	48 (61,5%)	17 (37%)	2 (20%)	16 (44,4%)	26 (57,8%)	13 (65%)	8 (61,5%)	23 (54,8%)	3 (30%)	-	38 (57,6%)	1 (100%)	11 (50%)	8 (47,1%)	4 (33,3%)	4 (57,1%)	31 (60,8%)	2 (28,6%)	5 (62,5%)
No, I do not know when my computer is hacked or infected and I don't know whom to contact.	10 (8,1%)	5 (6,4%)	5 (10,9%)	2 (20%)	1 (2,8%)	4 (8,9%)	2 (10%)	1 (7,7%)	5 (11,9%)	2 (20%)	-	3 (4,5%)	-	2 (9,1%)	1 (5,9%)	2 (16,7%)	-	3 (5,9%)	-	2 (25%)
Yes, I know when my computer is hacked or infected but I don't know whom to contact	13 (10,5%)	8 (10,3%)	5 (10,9%)	3 (30%)	5 (13,9%)	4 (8,9%)	1 (5%)	-	4 (9,5%)	2 (20%)	-	7 (10,6%)	-	3 (13,6%)	3 (17,6%)	-	-	7 (13,7%)	-	-
No, I do not know when my computer and I know whom to contact.	36 (29%)	17 (21,8%)	19 (41,3%)	3 (30%)	14 (38,9%)	11 (24,4%)	4 (20%)	4 (30,8%)	10 (23,8%)	3 (30%)	5 (100%)	18 (27,3%)	-	6 (27,3%)	5 (29,4%)	6 (50%)	3 (42,9%)	10 (19,6%)	5 (71,4%)	1 (12,5%)

Table 50: Non-ICT questionnaires - HESE responses to acknowledge of hacked or infected computer

Table 50 contains HESE non-ICT personnel responses to the following sentences/questions:

- Do you know when your computer is hacked or infected, and whom to contact when it occurs?

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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training institute (n=10)	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
Have you ever found a virus or Trojan on your computer at work?																				
Yes, my computer has been infected before	20 (16,1%)	14 (17,9%)	6 (13%)	-	8 (22,2%)	8 (17,8%)	2 (10%	2 (15,4%)	7 (16,7%)	-	1 (20%)	12 (18,2%)	-	2 (9,1%)	3 (17,7%)	2 (16,7%)	1 (14,3%)	9 (17,7%)	2 (28,6%)	1 (12,5%)
No, my computer has never been infected	81 (65,3%)	53 (68%)	28 (60,9%)	6 (60%)	24 (66,7%)	30 (66,7%)	15 (75%)	6 (46,2%)	27 (64,3%)	7 (70%)	3 (60%)	43 (65,2%)	1 (100%)	15 (68,2%)	11 (64,7%)	4 (33,3%)	4 (57,1%)	38 (74,5%)	4 (57,1%)	5 (62,5%)
I do not know what a virus or Trojan is	23 (18,6%)	11 (14,1%)	12 (26,1%)	4 (40%)	4 (11,1%)	7 (15,5%)	3 (15%)	5 (38,5%)	8 (19%)	3 (30%)	1 (20%)	11 (16,7%)	-	5 (22,7%)	3 (17,6%)	6 (50%)	2 (28,6%)	4 (7,8%)	1 (14,3%)	2 (25%)
Is anti-virus currently installed on your computer?																				
Yes	67 (54%)	44 (56,4%)	23 (50%)	4 (40%)	17 (47,2%)	25 (55,6%)	15 (75%)	6 (46,2%)	28 (66,7%)	4 (40%)	3 (60%)	31 (47%)	1 (100%)	12 (54,6%)	9 (52,9%)	5 (41,7%)	1 (14,3%)	31 (60,8%)	3 (42,9%)	6 (75%)
No	7 (5,7%)	3 (3,9%)	4 (8,7%)	-	3 (8,3%)	3 (6,7%)	-	1 (7,7%)	-	-	-	7 (10,6%)	-	1 (4,5%)	-	-	2 (28,6%)	4 (7,8%)	-	-
Do not know	50 (40,3%)	31 (39,7%)	19 (41,3%)	6 (60%)	16 (44,4%)	17 (37,8%)	5 (25%)	6 (46,2%)	14 (33,3%)	6 (60%)	2 (40%)	28 (42,4%)	-	9 (40,9%)	8 (47,1%)	7 (58,3%)	4 (57,1%)	16 (31,4%)	4 (57,1%)	2 (25%)
How careful are you when you open an attachment in email?																				
I always make sure it is from a person I know and I am expecting the email	59 (47,6%)	42 (53,8%)	17 (37%)	4 (40%)	17 (47,2%)	25 (55,6%)	9 (45%)	4 (30,8%)	21 (50%)	3 (30%)	1 (20%)	33 (50%)	1 (100%)	13 (59,1%)	7 (41,2%)	3 (25%)	3 (42,9%)	26 (51%)	3 (42,9%)	4 (50%)

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 long as I know the person or company that sent me the attachment, I open it	52 (41,9%)	30 (38,5%)	22 (47,8%)	3 (30%)	17 (47,2%)	14 (31,1%)	11 (55%)	7 (53,8%)	15 (35,7%)	4 (40%)	4 (80%)	29 (43,9%)	-	8 (36,4%)	8 (47,1%)	3 (25%)	4 (57,1%)	22 (43,1%)	4 (57,1%)	3 (37,5%)
There is nothing wrong with opening attachments	13 (10,5%)	6 (7,7%)	7 (15,2%)	3 (30%)	2 (5,6%)	6 (13,3%)	-	2 (15,4%)	6 (14,3%)	3 (30%)	-	4 (6,1%)	-	1 (4,5%)	2 (11,8%)	6 (50%)	-	3 (5,9%)	-	1 (12,5%)

Table 51: Non-ICT questionnaires - HESE responses to viruses and trojans recognition, usage of anti-virus programs and handling of email attachments

Table 51 contains HESE non-ICT personnel responses to the following sentences/questions:

- Have you ever found a virus or Trojan on your computer at work?
- Is anti-virus currently installed on your computer?
- How careful are you when you open an attachment in email?

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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training institute	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
Do you know what a social-engineering attack is?																				
Yes	45 (36,3%)	29 (37,2%)	16 (34,8%)	5 (50%)	21 (58,3%)	31 (68,9%)	12 (60%)	10 (76,9%)	14 (33,33%)	5 (50%)	3 (60%)	22 (33,3%)	1 (100%)	6 (27,3%)	6 (35,3%)	4 (33,3%)	4 (57,1%)	20 (39,2%)	3 (42,9%)	2 (25%)
No	79 (63,7%)	49 (62,8%)	30 (65,2%)	5 (50%)	15 (41,7%)	14 (31,1%)	8 (40%)	3 (23,1%)	28 (66,67%)	5 (50%)	2 (40%)	44 (66,7%)	-	16 (72,7%)	11 (64,7%)	8 (66,7%)	3 (42,9%)	31 (69,8%)	4 (57,1%)	6 (75%)
Do you know what an email scam is and how to identify one?																				
Yes, I know what an email scam is and how to identify one	46 (37,1%)	29 (37,2%)	17 (37%)	4 (40%)	15 (41,7%)	16 (35,6%)	6 (30%)	5 (38,5%)	17 (40,5%)	2 (20%)	-	27 (40,9%)	-	5 (22,7%)	7 (41,2%)	3 (25%)	2 (28,6%)	23 (45,1%)	2 (28,6%)	3 (37,5%)
I know what an email scam is, but I do not know how to identify one	48 (38,7%)	32 (41%)	16 (34,8%)	2 (20%)	15 (41,7%)	20 (44,4%)	8 (40%)	3 (23,1%)	12 (28,6%)	4 (40%)	5 (100%)	26 (39,4%)	1 (100%)	12 (54,5%)	4 (23,5%)	4 (33,3%)	4 (57,1%)	16 (31,4%)	5 (71,4%)	3 (37,5%)
No, I do not know what an email scam is or how to identify one	30 (24,2%)	17 (21,8%)	13 (28,3%)	4 (40%)	6 (16,7%)	9 (20%)	6 (30%)	5 (38,5%)	13 (30,9%)	4 (40%)	-	13 (19,7%)	-	5 (22,7%)	6 (35,3%)	5 (41,7%)	1 (14,3%)	12 (23,5%)	-	2 (25%)
My computer has no value to hackers, they do not target me.																				
True	33 (26,6%)	19 (24,4%)	14 (30,4%)	4 (40%)	11 (30,6%)	11 (24,4%)	2 (10%)	5 (38,5%)	12 (28,6%)	3 (30%)	3 (60%)	15 (22,7%)	-	6 (27,3%)	2 (11,8%)	6 (50%)	4 (57,1%)	11 (21,6%)	1 (14,3%)	3 (37,5%)
False	91 (73,4%)	59 (75,6%)	32 (69,6%)	6 (60%)	25 (69,4%)	34 (75,6%)	18 (90%)	8 (61,5%)	30 (71,4%)	7 (70%)	2 (40%)	51 (77,3%)	1 (100%)	16 (72,7%)	15 (88,2%)	6 (50%)	3 (42,9%)	40 (78,4%)	6 (85,7%)	5 (62,5%)

Table 52: Non-ICT questionnaires - HESE responses to social engineering attack acknowledge, email scam recognition and probability for being targeted from hackers

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 52 contains HESE non-ICT personnel responses to the following sentences/questions:

- Do you know what a social-engineering attack is?
- Do you know what an email scam is and how to identify one?
- My computer has no value to hackers, they do not target me.

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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training institute	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?																				
Yes	25 (20,2%)	15 (19,2%)	10 (21,7%)	2 (20%)	7 (19,4%)	7 (15,6%)	7 (35%)	2 (15,4%)	3 (7,1%)	2 (20%)	1 (20%)	18 (27,3%)	1 (100%)	8 (36,4%)	6 (35,3%)	3 (25%)	1 (14,3%)	3 (5,9%)	1 (14,3%)	3 (37,5%)
No	79 (63,7%)	53 (68%)	26 (56,5%)	4 (40%)	26 (72,2%)	29 (64,4%)	11 (55%)	9 (69,2%)	27 (64,3%)	5 (50%)	4 (80%)	43 (65,1%)	-	13 (59,1%)	9 (52,9%)	3 (25%)	5 (71,4%)	40 (78,4%)	6 (85,7%)	3 (37,5%)
Do not know	20 (16,1%)	10 (12,8%)	10 (21,7%)	4 (40%)	3 (8,3%)	9 (20%)	2 (10%)	2 (15,4%)	12 (28,6%)	3 (30%)	-	5 (7,6%)	-	1 (4,5%)	2 (11,8%)	6 (50%)	1 (14,3%)	8 (15,7%)	-	2 (25%)
Have you downloaded and installed software on your computer at work?																				
Yes	28 (22,6%)	16 (20,5%)	12 (26,1%)	2 (20%)	6 (16,7%)	11 (24,4%)	6 (30%)	3 (23,1%)	7 (16,7%)	1 (10%)	1 (20%)	18 (27,3%)	1 (100%)	5 (22,7%)	4 (23,5%)	4 (33,3%)	3 (42,9%)	6 (11,8%)	3 (42,9%)	3 (37,5%)
No	96 (77,4%)	62 (79,5%)	34 (73,9%)	8 (80%)	30 (83,3%)	34 (75,6%)	14 (70%)	10 (76,9%)	35 (83,3%)	9 (90%)	4 (80%)	48 (72,7%)	-	17 (77,3%)	13 (76,5%)	8 (66,7%)	4 (57,1%)	45 (88,2%)	4 (57,1%)	5 (62,5%)
Have you given your password to your colleagues or your manager, when you were asked for it?																				
Yes	32 (25,8%)	18 (23,1%)	14 (30,4%)	5 (50%)	13 (36,1%)	10 (22,2%)	3 (15%)	1 (7,7%)	14 (33,3%)	4 (40%)	1 (20%)	13 (19,7%)	-	3 (13,6%)	3 (17,6%)	5 (41,7%)	-	16 (31,4%)	1 (14,3%)	4 (50%)
No	92 (74,2%)	60 (76,9%)	32 (69,6%)	5 (50%)	23 (63,9%)	35 (77,8%)	17 (85%)	12 (92,3%)	28 (66,7%)	6 (60%)	4 (80%)	53 (80,3%)	1 (100%)	19 (86,4%)	14 (82,4%)	7 (58,3%)	7 (100%)	35 (68,6%)	6 (85,7%)	4 (50%)

Table 53: Non-ICT questionnaires - HESE responses to personal devices usage policies, employees' administrative rights on computers and password sharing

Table 53 contains HESE non-ICT personnel responses to the following sentences/questions:

- Can you use your own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential hospital information?
- Have you downloaded and installed software on your computer at work?
- Have you given your password to your colleagues or your manager, when you were asked for it?

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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training institute	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
Which of these is closer to your thinking, even if neither is exactly right?																				
Following security policies at our hospital prevents me from doing my job	30 (24,2 %)	13 (16,7%)	17 (37%)	3 (30%)	11 (30,6%)	10 (22,2%)	4 (20%)	2 (15,4%)	11 (26,2%)	4 (40%)	3 (60%)	12 (18,2%)	-	3 (13,6%)	2 (11,8%)	8 (66,7%)	2 (28,6%)	6 (11,8%)	5 (71,4%)	4 (50%)
Following security policies at our hospital helps me do my job better	94 (75,8 %)	65 (83,3%)	29 (63%)	7 (70%)	25 (69,4%)	35 (77,8%)	16 (80%)	11 (84,6%)	31 (73,8%)	6 (60%)	2 (40%)	54 (81,2%)	1 (100%)	19 (86,4%)	15 (88,2%)	4 (33,3%)	5 (71,4%)	45 (88,2%)	2 (28,6%)	4 (50%)
I feel I have been sufficiently trained in security at our hospital.																				
Strongly agree	3 (2,4%)	2 (2,6%)	1 (2,2%)	-	-	2 (4,4%)	-	1 (7,7%)	1 (2,4%)	1 (10%)	-	1 (1,5%)	-	1 (4,5%)	-	1 (8,3%)	-	1 (2%)	-	-
Agree	22 (17,7 %)	14 (17,9%)	8 (17,4%)	1 (10%)	5 (13,9%)	8 (17,8%)	6 (30%)	2 (15,4%)	7 (16,7%)	-	1 (20%)	13 (19,7%)	1 (100%)	6 (27,3%)	4 (23,5%)	-	-	9 (17,6%)	-	3 (37,5%)
Neither agree nor disagree	53 (42,7 %)	31 (39,7%)	22 (47,8%)	3 (30%)	18 (50%)	19 (42,2%)	6 (30%)	7 (53,8%)	21 (50%)	6 (60%)	2 (40%)	24 (36,4%)	-	5 (22,7%)	4 (23,5%)	7 (58,3%)	7 (100%)	24 (47,1%)	2 (28,6%)	4 (50%)
Disagree	36 (29%)	23 (29,5%)	13 (28,3%)	3 (30%)	9 (25%)	15 (33,3%)	6 (30%)	3 (23,1%)	10 (23,8%)	2 (20%)	2 (40%)	22 (33,3%)	-	8 (36,4%)	8 (47,1%)	2 (16,7%)	-	12 (23,5%)	5 (71,4%)	1 (12,5%)
Strongly disagree	10 (8,1%)	8 (10,3%)	2 (4,3%)	3 (30%)	4 (11,1%)	1 (2,2%)	2 (10%)	-	3 (7,1%)	1 (10%)	-	6 (9,1%)	-	2 (9,1%)	1 (5,9%)	2 (16,7%)	-	5 (9,8%)	-	-

Table 54: Non-ICT questionnaires - HESE responses to thoughts about following security policies and security training

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 54 contains HESE non-ICT personnel responses to the following sentences/questions:

- Following security policies at our hospital prevents me from doing my job OR Following security policies at our hospital helps me do my job better
- I feel I have been sufficiently trained in security at our 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.

	Total	Gender		Age					Education					Position						
	n = 124 (100 %)	Female (n=78)	Male (n=46)	21-30 (n=10)	31-40 (n=36)	41-50 (n=45)	51-60 (n=20)	>61 (n=13)	Secondary Education (n=42)	Vocational training institute (n=10)	Bachelor Degree (n=5)	MSc (n=66)	PhD (n=1)	Doctor (n=22)	Nurse (n=17)	Auxiliary personnel (n=12)	Lab. personnel (n=7)	Administrative personnel (n=51)	Technical personnel (n=7)	Other (n=8)
I am confident that I could recognize a security issue or incident if I saw one.																				
Strongly agree	5 (4%)	3 (3,8%	2 (4,3%)	-	1 (2,8%)	2 (4,4%)	-	2 (15,4%)	2 (4,8%)	-	-	3 (4,55%)	-	1 (4,5%)	1 (5,9%)	2 (16,7%)	-	1 (2%)	-	-
Agree	48 (38,7%)	31 (39,7%)	17 (37%)	4 (40%)	15 (41,7%)	14 (31,1%)	10 (50%)	5 (38,5%)	16 (38,1%)	4 (40%)	1 (20%)	26 (39,4%)	1 (100%)	9 (40,9%)	7 (41,2%)	-	1 (14,3%)	26 (51%)	2 (28,6%)	3 (37,5%)
Neither agree nor disagree	42 (33,9%)	24 (30,8%)	18 (39,1%)	3 (30%)	13 (36,1%)	17 (37,8%)	5 (25%)	4 (30,8%)	16 (38,1%)	5 (50%)	3 (60%)	18 (27,3%)	-	4 (18,2%)	2 (11,8%)	7 (58,3%)	6 (85,7%)	16 (31,4%)	3 (42,9%)	4 (50%)
Disagree	25 (20,2%)	18 (23,1%)	7 (15,2%)	2 (20%)	6 (16,7%)	12 (26,7%)	4 (20%)	1 (7,7%)	7 (16,7%)	1 (10%)	1 (20%)	16 (24,2%)	-	7 (31,8%)	6 (35,3%)	2 (16,7%)	-	7 (13,7%)	2 (28,6%)	1 (12,5%)
Strongly disagree	4 (3,2%)	2 (2,6%)	2 (4,3%)	1 (10%)	1 (2,8%)	-	1 (5%)	1 (7,7%)	1 (2,4%)	-	-	3 (4,55%)	-	1 (4,5%)	1 (5,9%)	1 (8,3%)	-	1 (2%)	-	-
Do you lock your PC when you leave your office even for a while?																				
Yes	95 (76,6%)	64 (82,1%)	31 (67,4%)	4 (40%)	30 (83,3%)	35 (77,8%)	18 (90%)	8 (61,5%)	28 (66,7%)	8 (80%)	5 (100%)	53 (80,3%)	1 (100%)	19 (86,4%)	13 (76,5%)	5 (41,7%)	5 (60%)	41 (80,4%)	6 (85,7%)	6 (75%)
No	29 (23,4%)	14 (17,9%)	15 (19,2%)	6 (60%)	6 (16,7%)	10 (22,2%)	2 (10%)	5 (38,5%)	14 (33,3%)	2 (20%)	-	13 (19,7%)	-	3 (13,6%)	4 (23,5%)	7 (58,3%)	2 (40%)	10 (19,6%)	1 (14,3%)	2 (25%)

Table 55: Non-ICT questionnaires - HESE responses to security issue recognition and PC locking when away from office

Table 55 contains HESE non-ICT personnel responses to the following sentences/questions:

- I am confident that I could recognize a security issue or incident if I saw one
- Do you lock your PC when you leave your office even for a while

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.