SECUREHOSPITALS.EU

RAISING AWARENESS ON CYBERSECURITY IN HOSPITALS ACROSS EUROPE AND BOOSTING TRAINING INITIATIVES DRIVEN BY AN ONLINE INFORMATION HUB

D4.3 New cybersecurity in hospitals curricula, materials and quality assurance report

This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

PROJECT DESCRIPTION

Acronym:	**SecureHospitals.eu**
Title:	**Raising Awareness on Cybersecurity in Hospitals across Europe and Boosting Training Initiatives Driven by an Online Information Hub**
Coordinator:	INTERSPREAD GmbH
Reference:	826497
Type:	CSA
Program:	HORIZON 2020
Theme:	eHealth, Cybersecurity
Start:	01. December, 2018
Duration:	26 months
Website:	https://project.securehospitals.eu/
E-Mail:	office@securehospitals.eu
Consortium:	**INTERSPREAD GmbH**, Austria (INSP), Coordinator **Erasmus Universiteit Rotterdam**, Netherlands (EUR) **TIMELEX**, Belgium (TLX) **Fundació Privada Hospital Asil de Granollers**, Spain (FPHAG) **Cooperativa Sociale COOSS Marche Onlus**, Italy (COOSS) **Arbeiter-Samariter-Bund**, Austria (SAM) **Johanniter International**, Belgium (JOIN) **European Aging Network**, Luxembourg (EAN)

DELIVERABLE DESCRIPTION

Number:	**D4.3**
Title:	**New cybersecurity in hospitals curricula, materials and quality assurance report**
Lead beneficiary:	**FPHAG**
Work package:	WP4
Dissemination level:	Public (PU)
Type	Report (R)
Due date:	30.09.2019
Submission date:	30.09.2019

Authors:

Marc Jofre, FPHAG
Javier Morate, FPHAG
Toni Alonso, FPHAG
Diana Navarro, FPHAG
Ramon Romeu, FPHAG

Contributors: **INSP, EUR, SAM, JOIN, TLX**

Reviewers: **Stela Shiroka,** INSP

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 826497.	**Disclaimer:** The content of this publication is the sole responsibility of the authors, and does not in any way represent the view of the European Commission or its services.

TABLE OF CONTENT

TABLE OF FIGURES

TABLE OF TABLES

EXECUTIVE SUMMARY

Based on the outcomes and the knowledge acquired in Work package 2 and 3, this work package encompasses the main outputs of the project in its initial stage: the creation of new training materials and definition of certain quality standards that all trainings on cybersecurity in hospitals should feature. The training materials created will serve for carrying out trainings of trainers and practitioners in the second project period. The rest of the material created in this work package will support the future of training on cybersecurity in hospitals in two ways: first by defining minimum requirements for training courses on cybersecurity in hospitals and second by creating guiding materials that support trainers develop tailor-made training courses. The needs for new course curricula and the quality standards will be developed on the basis of feedback from trainers and other cybersecurity experts.

The tasks defined in this work package are designed towards the achievement of Objective 3: '**CREATE** tailor-made training materials for trainers and IT practitioners to ensure the effective uptake of knowledge on data protection and privacy and cybersecurity measures.'

Achievements in this work package are marked with milestone M5.

Based on the feedback received by the trainers and related cybersecurity experts, this task 4.3 "**Create novel training curricula on cybersecurity in hospitals topics and define minimum quality standards for training material (Lead: FPHAG, Participants: EUR, INSP, SAM, JOIN, TLX)**" includes the creation of one of the main outputs of the projects: the course curricula that will be implemented in the multiple trainings. New training materials will be created to respond to the needs of the field but also certain quality standards for the training curricula and the trainer profiles (require qualifications of trainers) will be defined. All materials will be designed in the form of infographics and be disseminated widely across all available channels but primarily through the online hub.

1 Introduction

From previous work, in particular in T3.1 and T4.1, it is relevant that a little amount of training material, knowledge and courses are available for raising cybersecurity awareness for the medical sector. As shown in the previous tasks, most of the knowledge and course on cybersecurity awareness is focused for IT staff, while awareness should aim at all levels and roles in healthcare centres. Furthermore, from T3.3 "The trainer and relevant experts' feedback" enables the creation of materials for training as well as the definition of quality criteria that will be dealt with in this report.

There is a clear gap which this works starts to solve by providing an innovative new curriculum for cybersecurity awareness raising in healthcare centres.

As shown in Fig. 1, on the grounds of the knowledge provided by the collected EU policies and directives, publications and tools, the review of the existing courses and the inputs of trainers and training seekers, the next type of action within the project will be the creation of training materials and creation of solid grounds for higher quality trainings that address the most burning needs of IT practitioners in charge of patient data in healthcare settings. Novel training schemes and curricula will be developed and put in practice within various series of training activities within the project. Minimum required standards for the delivery of courses to trainers (train the trainer courses) and to practitioners of different levels, required qualifications for trainers and tools for supporting trainers online will be developed within this major action of creation.

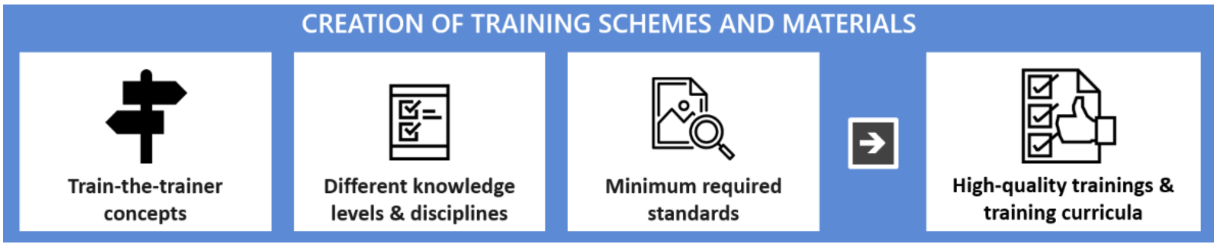

CREATION OF TRAINING SCHEMES AND MATERIALS
Train-the-trainer concepts
Different knowledge levels & disciplines
Minimum required standards
High-quality trainings & training curricula

FIGURE 1: Creation of new training curricula conceptualisation

In particular, in this deliverable the third box from the left is addressed by first assessing the different collected knowledge and disciplines in previous tasks to develop quality standard for new training curricula. Finally, the last box (rightmost box) is depicted by providing new cybersecurity curricula and material for hospitals.

On the grounds of the knowledge provided by the collected EU policies and directives, publications and tools, the review of the existing courses and the inputs of trainers and training seekers, the next type of action within the project is the creation of training materials and creation of solid grounds for higher quality trainings that address the most burning needs of IT practitioners in charge of patient data in healthcare settings. Novel training schemes and curricula are developed and put in practice within various series of training activities within the project. Minimum required standards for the delivery of courses to trainers (train the trainer courses) and to practitioners of different levels, required qualifications for trainers and tools for supporting trainers online are developed within this major action of creation.

Below, a summary of the procedure followed in **T4.3** "**New cybersecurity in hospitals curricula and materials and quality assurance report". Public report.**

1. Search literature and documentation on existing cybersecurity awareness raising curricula, materials and quality standards.
2. Describe the new curricula putting emphasis on the different staff profiles and roles. Defining a training package strategy and following a development guide.
3. Develop infographics with material focused to medical staff and non-medical staff in healthcare organizations.
4. Define quality standards and report.

1.1. Deliverable objectives

On the grounds of the knowledge provided by the collected EU policies and directives, publications and tools, the review of the existing courses and the inputs of trainers and training seekers, the next type of action within the project will be the creation of training material and creation of solid grounds for higher quality trainings that address the most burning needs of IT practitioners in charge of patient data in healthcare settings.

Novel training schemes and curricula will be developed and put in practice within various series of training activities within the project. Minimum required standards for the delivery of courses to trainers (train the trainer courses) and to practitioners of different levels, required qualifications for trainers and tools for supporting trainers online will be developed within this major action of creation.

1.2. Methodology

The methodology used for the elaboration of the novel curricula and quality standards for health cybersecurity pursues a series of objectives:

- To develop a document that is exhaustive, complete and reliable.
- To include information in a structured, standardized and intuitive way.
- Contribute to facilitating the work of comparing and cross-checking.
- Present it in as flexible and functional a format as possible. In such a way that represented, clearly and concisely the areas in which development and drive are.

To ensure that the information presented in this document is standardized, from the very beginning we opted for a descriptive file format to present the new curricula and quality standards develop, thus ensuring that the information follows the same structure for all items. Thus, the methodology used consists of four phases depicted in Fig. 1.

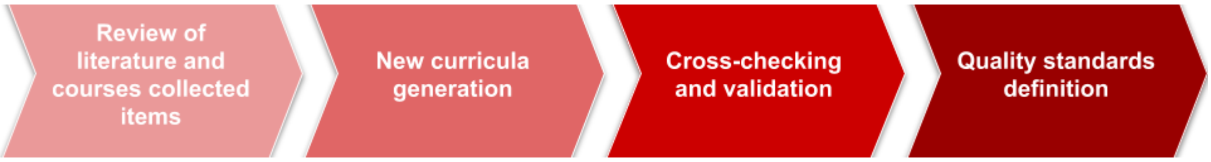

Review of literature and courses collected items
New curricula generation
Cross-checking and validation
Quality standards definition

FIGURE 2: Methodology steps for T4.3

2. Novel training curricula

In contrast to many other professions, medicine remains unique in that the majority of our training is devoted to perfecting one aspect (i.e. patient care) of the role, often leaving the skills needed to be a successful professional in today's business and political environments underdeveloped. Current healthcare policy remains in flux. Now more than ever, physicians need a centralized resource that is accessible and reliable to keep up with the changes; in particular, in cybersecurity.

One promising and innovative approach involves the development of a novel curriculum aimed at educating medical professionals on the key tenets of the European health care system affecting policy and cybersecurity [1-3]. The curriculum would ideally be an interactive, multidisciplinary course that is utilized longitudinally. It would be structured in a manner that does not leave healthcare policy by the neglected in medical education. The curriculum would produce medical professionals confident in navigating the challenges in health care.

However, it is increasingly difficult to find the time to learn beyond diseases and their treatments. An appropriate compromise could be to offer this novel curriculum on an elective basis. This follows the precedent set by many educational departments of Hospitals around Europe that offer optional electives (medical cybersecurity, etc.) for interested medical professionals to pursue.

If health care professionals are not able to tackle problems in their own profession due to a lack of knowledge, then the future of health care will be steered by unknown — and perhaps unqualified — entities. We contend that medical professionals are best suited to lead this change. In doing so, medical professionals will be able to advocate for policies that simultaneously improve their own career satisfaction and, most importantly, benefit patient care. A proposed solution consists of 4 elements intermeshed, but which are also fully effective if used separately, as described in Figure 3.

The baseline consists of quality standard and collection of training programs. The three pillars are: IT consultants providing technical knowledge, Health consultants providing medical knowledge and Trainers and Education consultants providing training knowledge.

Based on the quality standard, there are three pillars: IT consultants, health professionals and Trainers and Education consultants; which support the content of the curricula. On top, the Online Hub Platform informs about training solutions for cyber security awareness raising to IT staff, managers and health professionals, among others. Furthermore, it is innovative to align skills accompanied with knowledge, computer-based delivered programs and effectiveness training via learning-by-doing and relevant to the everyday work.

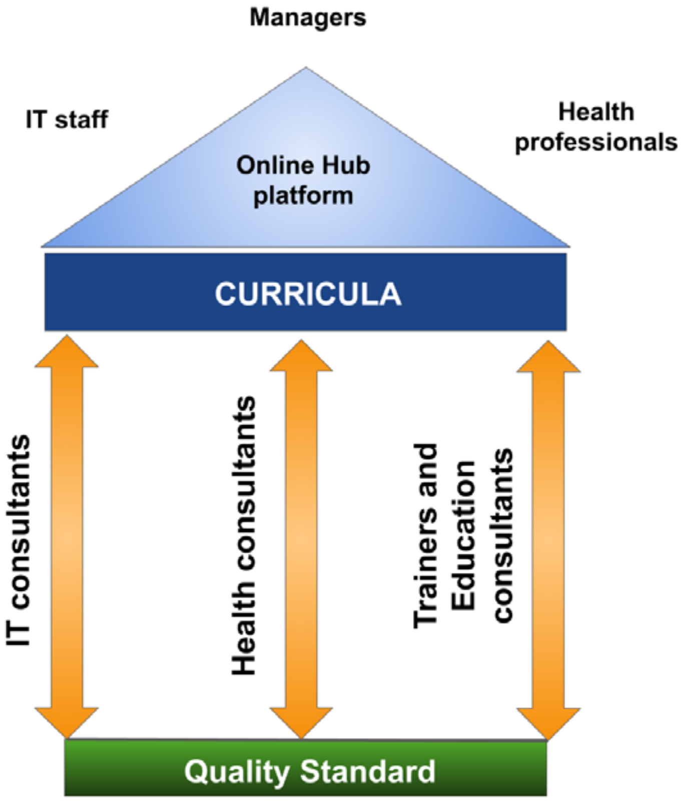


FIGURE 3: Novel training curricula diagram scheme

Already available medical cybersecurity awareness raising training programs (shown in Annex) where identified in T4.1. The existing gap in training programs for medical staff has been already identified: low amount of training programs for this staff group. Hence, it is relevant to identify the common topics presented in these training programs to asses in other appropriate tasks, the missing relevant topics for medical staff.

In particular, the topics already addressed by these training programs are focused on: a) personal data (PD) and health information (HI) regarded to terms as privacy, data protection, information to relatives and authorities. In addition, the other main topics covered in the collected training courses for medical staff are related to: b) EU GDPR and human factor in particular to the legal aspects related to them.

3. Medical training programs framework

Considering a general categorization description of the different roles of interest in a healthcare centre in terms of patients' data access level, the following categorization can be considered:

1. Digital information access level: Which staff role it could address or be useful for
   i. No access to patients' personal/clinical data (e.g. education, communication, finance, maintenance, human resources, research and innovation departments; mainly non-assistance staff).
   ii. Access to patients' personal data (e.g. administration staff).
   iii. Access to patients' clinical data (e.g. medical staff).
   iv. Access to aggregated personal/clinical data (Management team - CEO, CIO,...).
   v. Access to the source and all data (IT department).

3.1. Training packages strategy

Identification of most groups of practitioners categorized into patient's data access (taxonomy of roles – who we want to train) in Table 1.

Table 1: Taxonomy of roles

Staff role / Patient's data access	No access to personal/ clinical data	Access to personal data	Access to clinical data	Access to aggregated personal/ clinical data (Management)	Access to the source and all data (IT)
Kitchen, cleaning/laundry service	x				
Maintenance	x				
Human Resources	x	x			
Research and Innovation/ Education department /Library	x	(only anonymized)	(only anonymized)		
Stretchers/ Porter		x			
Storage and Logistics	x				

Private security staff	x				x
Clinical laboratory			x		
Pharmacy		x	x		
Radiology		x	x		
Pathologic Anatomy		x	x		
Administrative		x	x		
Medical Doctors		x	x		
Nursery		x	x		
IT staff		x	x		x
Accounting				x	
Management Team				x	
Head of Service or Supervisor		x	x	x	
Third party suppliers	x	x	x		x
Animators	x				
Call centre operators for home care services		x			x

Socio-sanitary operators		x	x		
Auxiliary Care staff		x			
Informal caregivers/relatives		x			x
Physiotherapists		x	x		
General practitioners		x	x		x
Psychologists		x	x		

Definition of possible scenarios [4,5] applying to each of the roles (what types of incidents they could be prone to), consequences of each of the scenarios and preventive measures for each of the behaviours and roles [6], are defined in Table 2. The list of threats is extracted from ENISA classification (https://etl.enisa.europa.eu/#/).

Table 2: Mitigation means for identified scenarios

Software platforms (entry point)	Threat / Patient's data access	No access to personal /clinical data	Access to personal data	Access to clinical data	Access to aggregated personal/clinical data (Management)	Access to the source and all data (IT)
e-mail	**Spam**	Identify and erase	Identify and erase	Identify and erase	Identify and erase. Support to buy new anti spam software	Identify and erase. Check / install anti spam software
e-mail, mobile app, sms	**Phishing**	Training, information	Training, information	Training, information	Training, information. Promote training programs	Training, information
web browsers	**Denial of Service**	N/A	N/A	N/A	Human and economic resources on IT. Know the thread.	Information, block the thread. Recovery techniques.

e-mail, mobile app, sms, usb devices/ network access by hacking firewall	**Cryptojacking**	Information and awareness	Information and awareness	Information and awareness	Information and awareness	Information, content filtering techniques
PC or mobile devices access	**Malware**	Information and awareness	Information and awareness	Information and awareness	Information and awareness	Information, block none wanted software. Check installed software
e-mail, mobile app, sms, usb devices/ network access by hacking firewall	**Ransomware**	Information and awareness	Information, awareness and training on safe documents	Information, awareness and training on safe documents	Information, awareness and training on safe documents. Promote training.	Provide safe repositories. Install backup and restore software
voice or video communication applications, printers, ftp and database access	**Cyber espionage**	Keep passwords. Protect screen. Don't leave PC unattended	Keep passwords. Protect screen. Don't leave PC unattended	Keep passwords. Protect screen. Don't leave PC unattended	Keep passwords. Protect screen. Do not leave PC unattended. Promote training	Password complexity rules. Screensavers. Audit logs on user actions
printers, public screens, wrong email directions, software development	**Information leakage**	Document destruction	Document destruction	Document destruction	Document destruction	Document destruction, check software leakage. Secure communications
outpatient box, public rooms, data centre	**Physical manipulation/ damage/ theft/ loss**	Be aware of suspicious behaviours	Be aware of suspicious behaviours	Be aware of suspicious behaviours. Don't leave areas unattended	Insurances. Limit access to sensitive areas. Hire security staff / security cameras.	Use of encryption. Inventories. Create user guides. Secure assets physically.
ID card, password leakage, e-mail, sms	**Identity theft**	Identify. Be aware of suspicious behaviours	Identify. Change password policy. Be aware of suspicious behaviours	Identify. Change password policy. Be aware of suspicious behaviours	Identify. Provide identity information. Promote training.	Identify. Secure access to applications. Provide identity information. Verify transactions. Strong and complex credentials.

						Filter content. Protect Wi-Fi connections
staff bribery, network access	**Data breaches (also negligent behaviour)**	Be aware of suspicious behaviours	Be aware of suspicious behaviours. Prevent data loss.	Be aware of suspicious behaviours. Prevent data loss. Apply data policies.	Classify data. Implement security policies. Data breach response plan. Promote training and awareness.	Data encryption. Apply data policies
e-mail, mobile app, sms, usb devices/ network access by hacking firewall	**Botnets**	N/A	N/A	N/A	Human and economic resources on IT. Know the thread.	Firewall. Traffic filtering. Regular updates. Network level controls
browser	**Web application attacks**	N/A	N/A	N/A	Human and economic resources on IT. Know the thread.	Security policies. Authentication and authorization. Traffic filtering. Input verification. Intrusion detection.
browser plugin	**Web-based attacks**	Do not install plugins on browsers.	Don't install plugins on browsers	Don't install plugins on browsers	Human and economic resources on IT. Know the thread.	Regular patches and updates. Web traffic encryption. Control web plugins. Prevent user to install plugins or change browser configuration
HIS, database access	**Inside threat**	Training and awareness	Training and awareness	Training and awareness	Security policies. Access levels. Promote training.	Behaviour analysis tools. Identity management solutions. Audit and log user actions. Role-based access control

The framework for the different staff roles [7-9]. Filling the gap of IT / health / training topics in audience vs. complexity level matrix, is defined in Table 3.

Table 3: Framework of training curricula for the different staff roles

Complexity level	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Beginner	Definition: Spam, phishing, malware, ransomware, cyber espionage, information leakage Be aware of suspicious behaviours. Prevent data loss. Introduction to GDPR (detect and respond to data breaches).	Definition: Spam, phishing, malware, ransomware, cyber espionage, information leakage. Be aware of suspicious behaviours. Prevent data loss. Do not leave areas unattended. Introduction to GDPR (data minimization, data subject rights; principles).	Definition: Spam, phishing, malware, ransomware, cyber espionage, information leakage. Be aware of suspicious behaviours. Prevent data loss. Do not leave areas unattended. Introduction to GDPR (principles and theory of handling data subject requests, data protection, impact assessment and data breaches procedures; accountability requirements).	Basic concepts of all threats and GDPR (technical measures required).
Advanced	Definition: cryptojacking, ransomware, identity theft, data breaches. Plugins on browsers. Identify and complex credentials. Compliance to GDPR.	Definition: cryptojacking, ransomware, identity theft, data breaches. Agents involved in cybersecurity Plugins on browsers. Identify and complex credentials. Compliance to GDPR.	Definition: cryptojacking, ransomware, identity theft, data breaches. Agents involved in cybersecurity Identify. Provide identity information Limit access to sensitive areas. Plugins on browsers. Promote training. Compliance to GDPR (real scenarios/use cases of handling data subject	Spam: anti-spam software Denial of Services Cryptojacking ransomware Information leakage. Creation of safe repositories Firewall. Identify. Web traffic encryption Configure browser. Identity management solutions Audit and log user actions. Strong and complex credentials. Intermediate Compliance to GDPR.

			requests, how to make protection data impact assessment and who to involve).	
Expert	If interested same concepts as Management Expert	If interested same concepts as Management Expert.	Denial of services: definition Insurances Security policies. Access levels. Expertise in GDPR ((real scenarios/use cases of handling data subject requests, how to make protection data impact assessment and who to involve).	Secure access to applications. Traffic filtering. Network level controls. Security policies. Authentication and authorization. Intrusion detection. Behaviour analysis tools. Protect Wi-Fi connections. Expertise in GDPR.

3.2. Relevant cases

1. Ransomware + Phishing:

A kitchen staff member received a personal mail in the email inbox. This mail pretended to be a mail from the postal delivery service. The mail said that they had to click some link to know about an in-route package. By clicking on the link, a program was downloaded and executed in the computer. At that moment, a malicious program began to encrypt documents and spread all over the network. Then, when the program had already infected some other computers and encrypted a lot of documents, a pop-up screen was shown with instructions to pay a ransom to recover the encrypted documents.

Table 4: Relevant cases: Ransomware + Phishing

Staff role	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Recommendations	First, many people on staff may not know enough about ransomware and how it works, so the primary task is general awareness.	However, we know that hospital staff members are often busy and under time pressure, so ensuring that each person has read the entire article and understood what	To that effect, IT has written several articles on ransomware including its history and methods, which could be sent out to all employees.	That is why there is a second step that can quickly illuminate who in the organization is more prone to an accidental click.

		they need to do to protect themselves can be a challenge in and of itself.		
Training level	Expert	Expert	Advanced	Beginner

2. Information leakage:

A Medical Doctor printed a document with personal and clinical data and forgot it on the desk. Then a cleaning service person grabbed the document and checked it, realizing that the patient was a relative.

Table 5: Relevant cases: Information leakage

Staff role	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Recommendations	Always use anonymized information as much as possible	Establish a culture of less printing and instead use more digital documents.	Those who organize the information infrastructure and facilitate the work of others must set a good example.	Spread culture of privacy and confidentiality. Sensitive information on a desk such as sticky notes, papers and printouts can easily be taken by thieving hands and seen by prying eyes. All sensitive and confidential information should be removed from the desk at the end of each working day.
Training level	Beginner	Beginner	Beginner	Beginner

3. Information leakage + Theft

USB stick with clinical and personal data left in the outpatient box and the patient took it home. Maybe the patient only wanted the USB memory for its storage value, not for its contents, but the fact is that it was stolen and not knowing what the patient did with the data.

Table 6: Relevant cases: Information leakage + Theft

Staff role	Non-medical (no access to clinical nor personal	Medical (access to clinical and/or	Management (access to	IT (access to the source and all

	patient's data)	personal patient's data)	aggregated clinical and personal patient's data)	clinical and personal patient's data)
Recommendations	All devices containing Health Information are inventoried and can be accounted for.	Sensitive information on a desk such as sticky notes, papers and printouts can easily be taken by thieving hands and seen by prying eyes. All sensitive and confidential information should be removed from the desk at the end of each working day.	Your corporate personnel must be educated about the menaces of unsolicited removable media and prohibited from accessing any stray media such as an external hard drive, even if it is on a secured system.	Once you learn what the issues are, take tangible steps to address them. Work to make simple fixes that can have a big impact, such as shortening wait times and improving customer service. It is also important to invest in training and development workshops for clinical staff.
Training level	Beginner	Beginner	Advanced	Advanced

4. Data breaches + Inside threat:

A VIP person was hospitalized. A gossip magazine wanted to know some information about that person. Therefore, they bribed an employee to get the patient's personal and clinical data. Shortly, the yellow press started publishing gossip, fake news about the VIP's health. The VIP sued the hospital and a bad reputation for the hospital was generated.

Table 7: Relevant cases: Data breaches + Inside threat

Staff role	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Recommendations	Have very clear policies and understanding of GDPR.	Promote honourable practices and procedures (do the right thing).	Setting file access permissions may be done manually, using an access control list. Someone with authorized rights to the system can only do this. Prior to setting these permissions, it is important to identify which files	Every user account can be positively tied to a currently authorized individual. Users are only authorized to access the information they need to perform their duties.

			should be accessible to which staff members.	
Training level	Advanced	Advanced	Beginner	Expert

5. Identity theft:

During some maintenance works in the IT department, the data centre was a crowded place. A fake maintenance staff person was detected inside the data centre. A member of the IT department called security to identify and stop that person. The suspicious person was detained and explained that changed worker clothes with another IT staff worker, which generated confusion to the point that big security breach could have affected the hospital.

Table 8: Relevant cases: Identity theft

Staff role	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Recommendations	Physical access to secure areas is limited to authorized individuals.	All devices containing Health Information are inventoried and can be accounted for.	Have in place ISO policy (e.g. ISO 27000 family).	Securing information physically should include policies limiting physical access, e.g. Securing machines in locked rooms, managing physical keys, and restricting the ability to remove devices from a secure area.
Training level	Beginner	Beginner	Expert	Advanced

6. Data breaches + Inside threat + Cyber espionage

A medical doctor was fired and copied into a USB device all patient data to later use it at the private clinic. The medical doctor allegedly created a folder called 'Patients' on the laptop containing 'private, confidential and sensitive medical records' of regular patients, then later copied it to a portable data storage USB stick. However, the medical doctor, branded the claims 'vague and embarrassing', insisting [the medical doctor] only took copies of the patient's records to help 'tidy' the electronic files when leaving.

Table 9: Relevant cases: Data breaches + Inside threat + Cyber espionage

Staff role	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Recommendations	Basic legal knowledge related to work environments.	Have GDPR knowledge related to personal data and health information.	Have in place an IT staff exit policy for staff resignation or retirement.	Educating the hospital's top management about the impact of poor security and its consequences on staff retention will help.
Training level	Expert	Expert	Advanced	Expert

7. Denial of Service + Web application attacks:

During some political event that happened at the hospital's territory, the political counterpart tried to cause chaos among the population. The hospital's websites were attacked with Denial of Service (DoS) and they tried to discover data web services, in order to collapse or deactivate them.

Table 10: Relevant cases: Denial of Service + Web application attacks

Staff role	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Recommendations	Update and maintain computer software updated.	It is better to disable pop-up windows, as they invite risks. Users should refrain from installing software programs from unknown sources, especially links infected with malware. Many websites offer free Internet security programs that infect your system rather than protecting it.	Assessment of hospital's firewalls and security measures as well as review of security levels of third party networks to which the hospital's network is connected.	Establishing a cybersecurity response team that can quickly act when an attack is detected so that the damage can be minimized.
Training level	Beginner	Beginner	Expert	Expert

8. Cryptojacking:

A nursery person called IT technical support, claiming that her PC was running very slow. The IT helpdesk operator connected to the computer and realized that, indeed, the computer was very slow, without an obvious reason or running any heavy program, just an Internet browser. In addition, strange behavior was detected: when the browser was closed, the computer worked normally and when it was running, the computer started to slow down again. In the IT department, they realized that a cryptojacking program was exploiting a security breach in a browser add-on previously installed on this particular computer. When the add-on was disabled, the cryptojacking software could not take advantage of the security breach of the plugin and stopped its activity.

Table 11: Relevant cases: Cryptojacking

Staff role	Non-medical (no access to clinical nor personal patient's data)	Medical (access to clinical and/or personal patient's data)	Management (access to aggregated clinical and personal patient's data)	IT (access to the source and all clinical and personal patient's data)
Recommendations	All staff members know how to recognize possible symptoms of viruses or malware on their computers.	Therefore, do not just assume your IT department has a handle on the problem. (In addition, if you are reading this and are in healthcare IT, you know you are not as prepared as you should be.) Instead, take matters into your hands and schedule a meeting to discuss the necessary steps to better strengthen the entire network's security	Making equipment on the network difficult to identify so that hackers cannot quickly hone in on highly vulnerable machines/ equipment to cause a disruptive attack.	Employees should learn how to identify malware and what to do if their device or network has been infected. The immediate response should be to turn off the system or device and inform the security management team.
Training level	Advanced	Advanced	Expert	Advanced

3.3. Collected materials

For the different digital information access level, some material is shown in Table 2.

Table 12: Available material for different digital information access level roles

Digital information access level	Main points to address	Materials

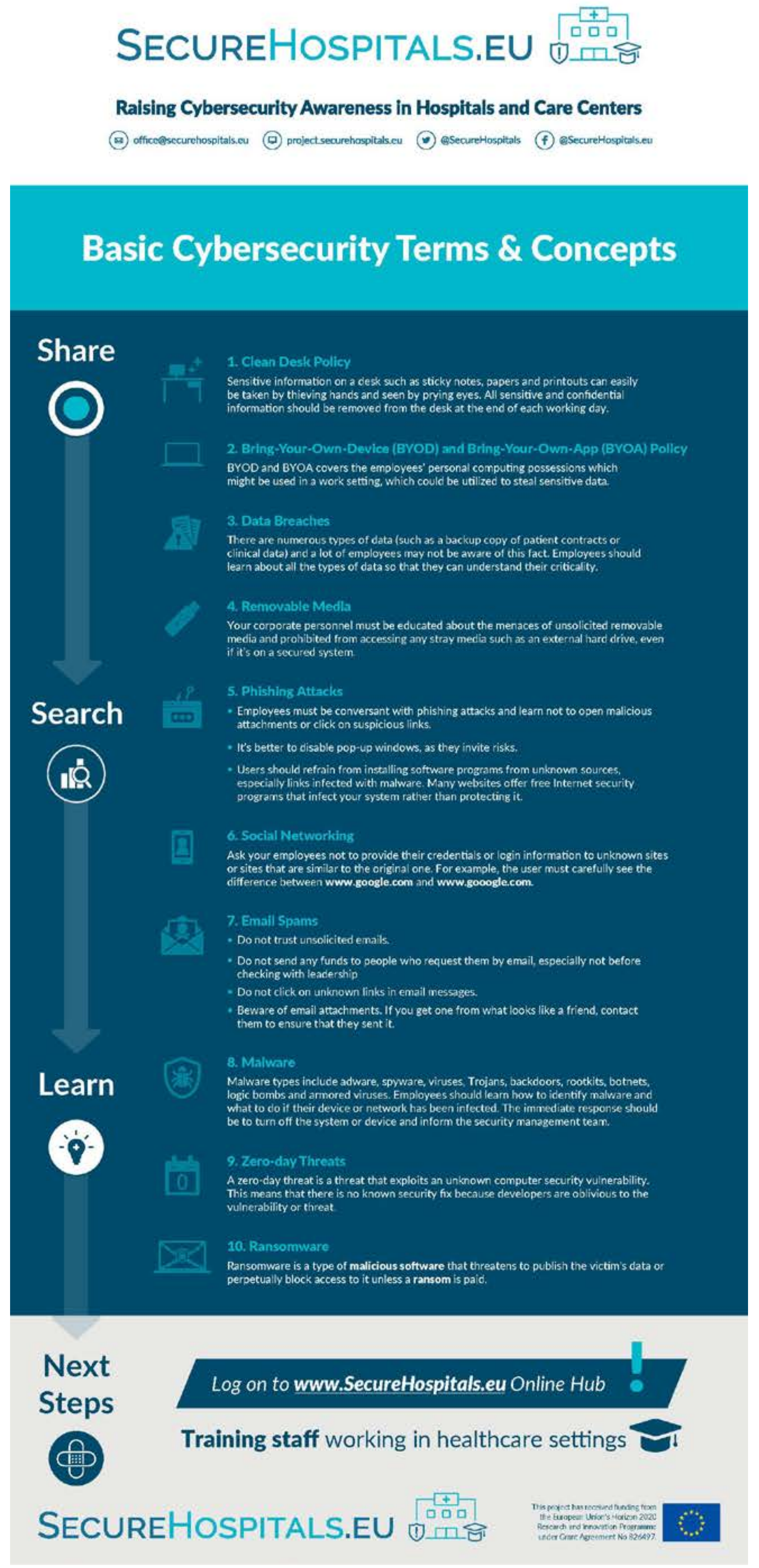
No access to patients' clinical/personal data	It is important that the personnel involved in the third-party communications process understand how the security of the information shared with third parties can be impacted and the role the third parties play in the security awareness program.	European Cyber Security Month 2018 - Cyber Security is a Shared Responsibility: https://www.youtube.com/watch?v=ZlxR6nBYCLM Cyber awareness challenge 2019: https://iatraining.disa.mil/eta/cyber-awareness-challenge/launchPage.htm Social Networking: https://iatraining.disa.mil/eta/disa_sn_v21_fy17/launchPage.htm
Access to patients' personal data	Personnel in these roles are often the "first line of defense" as they are interacting directly with patients' data. Training for this role may include how to be on the lookout for suspicious behaviour in areas where the public has access to appointment terminals.	#CyberSecMonth: https://www.youtube.com/results?search_query=%23CyberSecMonth 2017 - Skills in Cyber Security: https://www.youtube.com/watch?v=s3IolOd6JeA Mobile Devices: https://iatraining.disa.mil/eta/disa_mobile_v11_fy17/launchPage.htm Phishing Awareness: https://iatraining.disa.mil/eta/phishing-awareness/launchPage.htm
Access to patients' clinical data	Medical staff will need to understand security requirements enough to discuss and reinforce them, and encourage personnel to follow the requirements. Medical staff that is security-aware better understands the risk factors to the organization's information. This knowledge helps them make well-informed decisions related to medical operations.	Cybersecurity in the workplace: https://www.youtube.com/watch?v=1cFNhvm-np0&t=1s Identifying and Safeguarding Personal Data (PD): https://iatraining.disa.mil/eta/disa_mobile_v11_fy17/launchPage.htm Identifying and Safeguarding Health Data (HD): https://iatraining.disa.mil/eta/personally-identifiable-information-pii/launchPage.htm
Access to patients' aggregated clinical and personal data (Management)	In addition to content for all personnel, management training should include more detailed information regarding the consequences of a breach to management stakeholders. Management should understand not only the monetary penalties of failing to safeguard, but also the lasting harm to the organization due to reputational (brand) damage. This factor is often overlooked when organizations outsource payment processing, but is critically important. Managers who are security-aware can also assist with the development of data	European Cyber Security Month 2018 - Teaser: https://www.youtube.com/watch?v=vWNUHaxensE Best Practices for Victim Response and Reporting of Cyber Incidents https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf Assurance for senior leaders:

	security policies, secure procedures, and security awareness training.	https://iatraining.disa.mil/eta/ma-srleaders/launchpage.htm
Access to the source and all patients' data (IT)	IT administrators and Developers System, Database, and Network Administrators and other staff with privileged access to computer systems that may store, process, or transmit data will require more detailed security awareness training that includes understanding the importance of secure system configurations for the protection of sensitive information. Application developers, system developers, and testing staff have access to underlying code base, which is critical to environment security. These users should be aware of their responsibilities to follow the organization's security policy, secure coding practices, change control procedures, and be aware of current information on security threats and effective countermeasures.	Governance, Privacy & Data Protection: https://www.youtube.com/watch?v=L2DqWvfsBR8 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf Using public key infrastructure (PKI): https://iatraining.disa.mil/eta/using_pki/launchpage.htm
All staff roles	Inside threats contribute the most to breaches. This can be due to ignorance or conscious mishandling data. Hospitals should establish a cybersecurity culture/department and raise awareness towards the issue. Frequent employee training, maintaining good computer habits and do's and don'ts of handling patients' data should be long-term projects within all institutions.	Material for raising information security awareness: https://cybersecuritymonth.eu/press-campaign-toolbox/material Cybersecurity resources: https://cybersecuritymonth.eu/references/partners-resources/resources#c7=effective&b_start=0 European Cyber Security Month - NIS Quiz: https://cybersecuritymonth.eu/references/quiz-demonstration/intro Educational example infographics: https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/nis-brokerage-1/nis-in-education-infographics RRI examples according to profile: https://www.rri-tools.eu/how-tos ENISA threat landscape: https://etl.enisa.europa.eu NCSC glossary infographic: https://www.ncsc.gov.uk/blog-post/download-latest-ncsc-glossary-infographic

From the previous available material, we believe that a missing part of material is specifically for healthcare institutions targeted to medical staff. As a beginning work, several infographics for use in healthcare institutions focused to the specific different identified roles are developed and shown below.

3.4. Infographics

Several new materials have been generated in the format of infographics, that will be utilised as materials for the workshops as trainings, and also for raising awareness online through the project's communication channels. The intensive awareness raising campaign for which the materials will be utilised starts in October, matching with the Cyber Security Month initiative of the EU.



SECUREHOSPITALS.EU

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu | project.securehospitals.eu | @SecureHospitals | @SecureHospitals.eu

Basic Cybersecurity Terms & Concepts

Share

1. Clean Desk Policy

Sensitive information on a desk such as sticky notes, papers and printouts can easily be taken by thieving hands and seen by prying eyes. All sensitive and confidential information should be removed from the desk at the end of each working day.

2. Bring-Your-Own-Device (BYOD) and Bring-Your-Own-App (BYOA) Policy

BYOD and BYOA covers the employees' personal computing possessions which might be used in a work setting, which could be utilized to steal sensitive data.

3. Data Breaches

There are numerous types of data (such as a backup copy of patient contracts or clinical data) and a lot of employees may not be aware of this fact. Employees should learn about all the types of data so that they can understand their criticality.

4. Removable Media

Your corporate personnel must be educated about the menaces of unsolicited removable media and prohibited from accessing any stray media such as an external hard drive, even if it's on a secured system.

Search

5. Phishing Attacks

- Employees must be conversant with phishing attacks and learn not to open malicious attachments or click on suspicious links.
- It's better to disable pop-up windows, as they invite risks.
- Users should refrain from installing software programs from unknown sources, especially links infected with malware. Many websites offer free Internet security programs that infect your system rather than protecting it.

6. Social Networking

Ask your employees not to provide their credentials or login information to unknown sites or sites that are similar to the original one. For example, the user must carefully see the difference between **www.google.com** and **www.gooogle.com**.

7. Email Spams

- Do not trust unsolicited emails.
- Do not send any funds to people who request them by email, especially not before checking with leadership
- Do not click on unknown links in email messages.
- Beware of email attachments. If you get one from what looks like a friend, contact them to ensure that they sent it.

Learn

8. Malware

Malware types include adware, spyware, viruses, Trojans, backdoors, rootkits, botnets, logic bombs and armored viruses. Employees should learn how to identify malware and what to do if their device or network has been infected. The immediate response should be to turn off the system or device and inform the security management team.

9. Zero-day Threats

A zero-day threat is a threat that exploits an unknown computer security vulnerability. This means that there is no known security fix because developers are oblivious to the vulnerability or threat.

10. Ransomware

Ransomware is a type of **malicious software** that threatens to publish the victim's data or perpetually block access to it unless a **ransom** is paid.

Next Steps

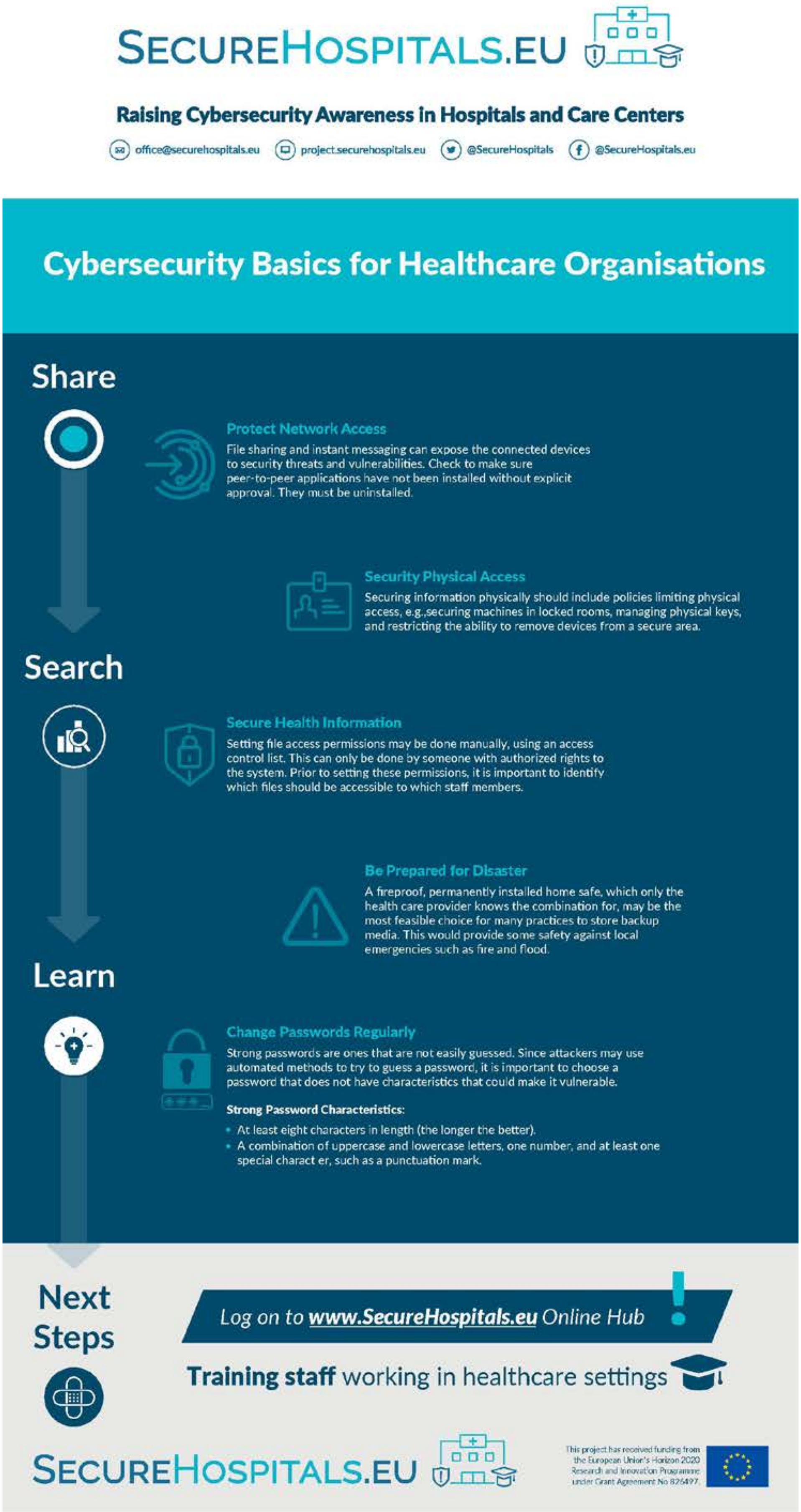
*Log on to **www.SecureHospitals.eu** Online Hub*

Training staff working in healthcare settings

SECUREHOSPITALS.EU

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

FIGURE 4: Infographic No. 1: Cybersecurity information for Healthcare - General concepts



SECUREHOSPITALS.EU

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu project.securehospitals.eu @SecureHospitals @SecureHospitals.eu

Cybersecurity Basics for Healthcare Organisations

Protect Network Access

File sharing and instant messaging can expose the connected devices to security threats and vulnerabilities. Check to make sure peer-to-peer applications have not been installed without explicit approval. They must be uninstalled.

Security Physical Access

Securing information physically should include policies limiting physical access, e.g.,securing machines in locked rooms, managing physical keys, and restricting the ability to remove devices from a secure area.

Secure Health Information

Setting file access permissions may be done manually, using an access control list. This can only be done by someone with authorized rights to the system. Prior to setting these permissions, it is important to identify which files should be accessible to which staff members.

Be Prepared for Disaster

A fireproof, permanently installed home safe, which only the health care provider knows the combination for, may be the most feasible choice for many practices to store backup media. This would provide some safety against local emergencies such as fire and flood.

Change Passwords Regularly

Strong passwords are ones that are not easily guessed. Since attackers may use automated methods to try to guess a password, it is important to choose a password that does not have characteristics that could make it vulnerable.

Strong Password Characteristics:

- At least eight characters in length (the longer the better).
- A combination of uppercase and lowercase letters, one number, and at least one special charact er, such as a punctuation mark.

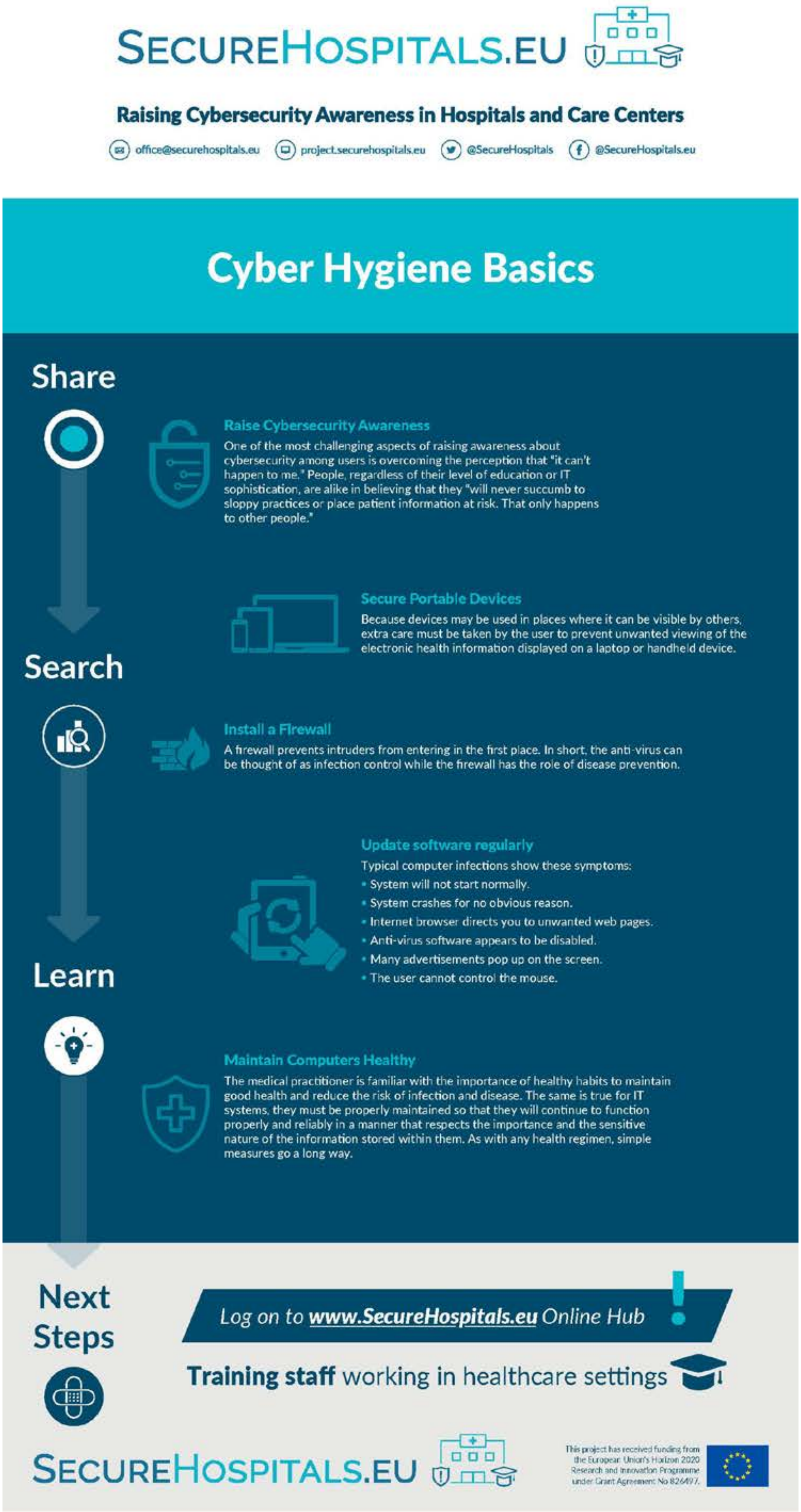
Log on to www.SecureHospitals.eu Online Hub

Training staff working in healthcare settings

SECUREHOSPITALS.EU

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

Figure 5: Infographic No. 2: Cybersecurity information for Healthcare - General recommendations



SECUREHOSPITALS.EU

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu project.securehospitals.eu @SecureHospitals @SecureHospitals.eu

Cyber Hygiene Basics

Share

Search

Learn

Raise Cybersecurity Awareness

One of the most challenging aspects of raising awareness about cybersecurity among users is overcoming the perception that "it can't happen to me." People, regardless of their level of education or IT sophistication, are alike in believing that they "will never succumb to sloppy practices or place patient information at risk. That only happens to other people."

Secure Portable Devices

Because devices may be used in places where it can be visible by others, extra care must be taken by the user to prevent unwanted viewing of the electronic health information displayed on a laptop or handheld device.

Install a Firewall

A firewall prevents intruders from entering in the first place. In short, the anti-virus can be thought of as infection control while the firewall has the role of disease prevention.

Update software regularly

Typical computer infections show these symptoms:

- System will not start normally.
- System crashes for no obvious reason.
- Internet browser directs you to unwanted web pages.
- Anti-virus software appears to be disabled.
- Many advertisements pop up on the screen.
- The user cannot control the mouse.

Maintain Computers Healthy

The medical practitioner is familiar with the importance of healthy habits to maintain good health and reduce the risk of infection and disease. The same is true for IT systems, they must be properly maintained so that they will continue to function properly and reliably in a manner that respects the importance and the sensitive nature of the information stored within them. As with any health regimen, simple measures go a long way.

Next Steps

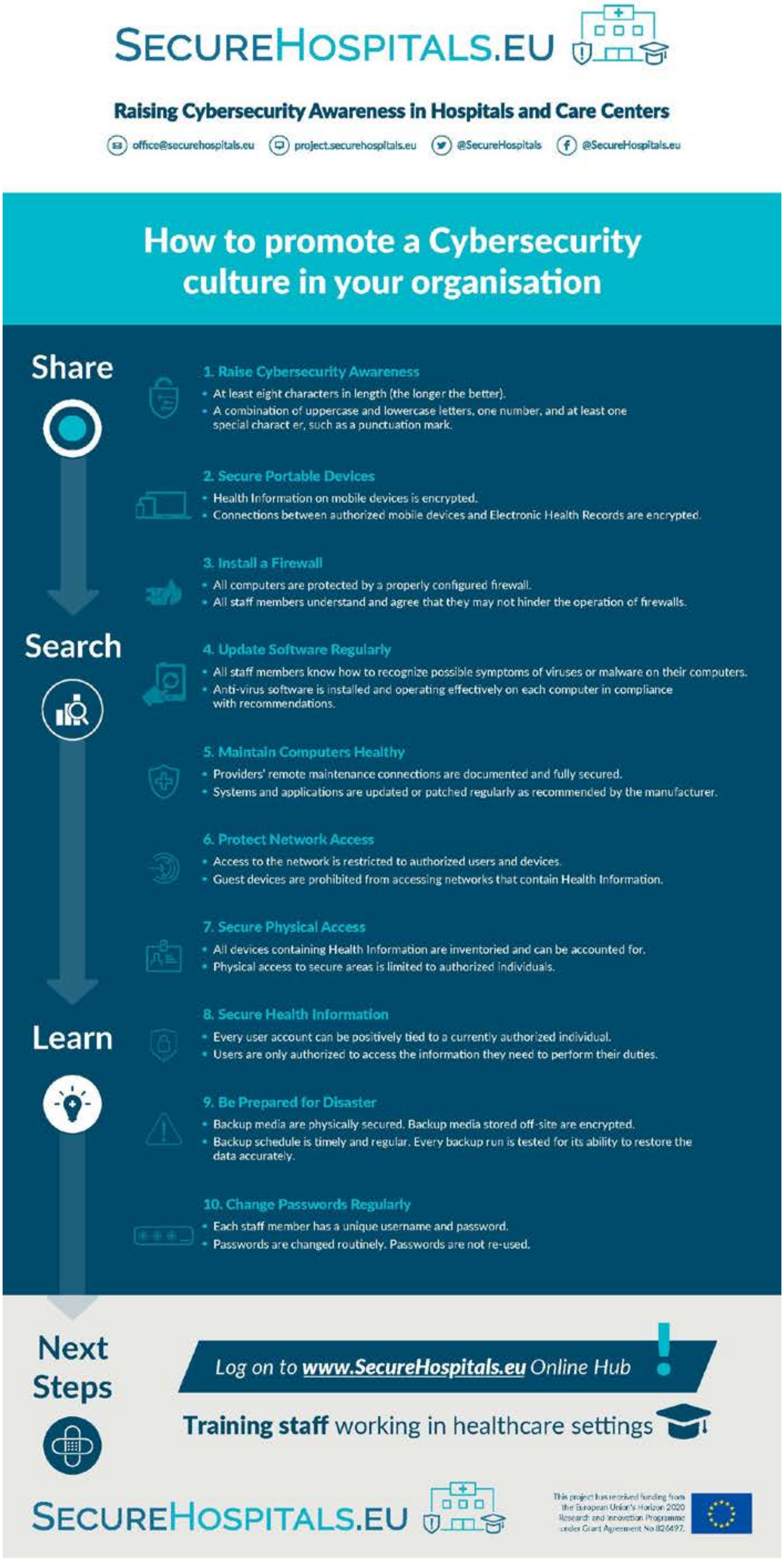
Log on to **www.SecureHospitals.eu** Online Hub

Training staff working in healthcare settings

SECUREHOSPITALS.EU

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

FIGURE 6: Infographic No. 3: Cybersecurity information for Healthcare - General recommendations



SECUREHOSPITALS.EU

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu project.securehospitals.eu @SecureHospitals @SecureHospitals.eu

How to promote a Cybersecurity culture in your organisation

1. Raise Cybersecurity Awareness

- At least eight characters in length (the longer the better).
- A combination of uppercase and lowercase letters, one number, and at least one special charact er, such as a punctuation mark.

2. Secure Portable Devices

- Health Information on mobile devices is encrypted.
- Connections between authorized mobile devices and Electronic Health Records are encrypted.

3. Install a Firewall

- All computers are protected by a properly configured firewall.
- All staff members understand and agree that they may not hinder the operation of firewalls.

4. Update Software Regularly

- All staff members know how to recognize possible symptoms of viruses or malware on their computers.
- Anti-virus software is installed and operating effectively on each computer in compliance with recommendations.

5. Maintain Computers Healthy

- Providers' remote maintenance connections are documented and fully secured.
- Systems and applications are updated or patched regularly as recommended by the manufacturer.

6. Protect Network Access

- Access to the network is restricted to authorized users and devices.
- Guest devices are prohibited from accessing networks that contain Health Information.

7. Secure Physical Access

- All devices containing Health Information are inventoried and can be accounted for.
- Physical access to secure areas is limited to authorized individuals.

8. Secure Health Information

- Every user account can be positively tied to a currently authorized individual.
- Users are only authorized to access the information they need to perform their duties.

9. Be Prepared for Disaster

- Backup media are physically secured. Backup media stored off-site are encrypted.
- Backup schedule is timely and regular. Every backup run is tested for its ability to restore the data accurately.

10. Change Passwords Regularly

- Each staff member has a unique username and password.
- Passwords are changed routinely. Passwords are not re-used.

Log on to ***www.SecureHospitals.eu*** *Online Hub*

Training staff working in healthcare settings

SECUREHOSPITALS.EU

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

FIGURE 7: Infographic No. 4: Cybersecurity information for Healthcare - General recommendations

3.5. Relation to D3.4

In Table 13, it is related the training curricula and materials indicated in the previous sections to D3.4 Baseline report and training materials. The D3.4 Baseline report regards the information collected and delivered in task 3.4 as the development of a baseline report in the form of a handbook that sorts the information in a concise for its inclusion on the online hub.

Table 13: Relation of training curricula and materials indicated in previous sections to D3.4

Baseline Report	Article	Summary	Threat	Data Access
Policies and Regulations	NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	N.A.	All roles
	eIDAS Regulation	Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	N.A.	All roles
	GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	N.A.	All roles
	ISO/IEC 27000 family	Description of the ISO/IEC 27000 family on information security management systems	N.A.	All roles
	National cybersecurity plans	Clarification and examples of national cybersecurity plans	N.A.	All roles
	Medical Devices Regulation and In-Vitro Diagnosis Devices Regulation	Regulation 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/ECC Regulation (EU) 2017/746 of	N.A.	All roles

		the European Parliament and if the Council of 5 April 2017 on in-vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU		
	Cybersecurity Act	Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity)	N.A.	All roles
	CSIRT Network and its members	Description of the Computer Security Incident Response Team Network and its members	N.A.	All roles
Handbooks & Guidelines	How to create strong password	With the amount of websites for which you probably have accounts, there is no simple way to easily remember every single password without duplicating passwords or utilizing some sort of pattern.	Cyber espionage, Identity theft, Inside threat	All roles
	Habits to be safe online	Cyber hygiene, or habits to be safe online, is related to the practices and steps that computer or device users do to maintain information safety and improve online security. These practices are often part of a routine to ensure the security of identity and other information that could be stolen or harmed.	All threats	All roles
	Cybersecurity management guidelines	In the global race for economic competitiveness, the digital readiness of economies has become a key factor. Therefore, cybersecurity has become an increasingly important safety issue. In addition, cybercrime has shifted from attacking big corporations to also attack other industries, like financial services and especially the health sector.	All threats	Management
	Ransomware: risks and preventive actions	Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a	Ransomwa re	All roles

		ransom is paid.		
	Good Practice Guide for Incident Management, ENISA (https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management)	This guide complements the existing set of ENISA guides that support Computer Emergency Response Teams. It describes good practices and provides practical information and guidelines for the management of network and information security incidents with an emphasis on incident	All threats	All roles
	Incident Handler's Handbook, SANS Institute (https://www.sans.org/reading-room/whitepapers/incident/paper/3390)	One of the greatest challenges facing today's IT professionals is planning and preparing for the unexpected, especially in response to a security incident. The scope of this document is limited to the six phases of the incident handling process ("Incident handling step---by---step," 2011) and providing the basic information necessary as to what each step entails.	All threats	IT
	Materials and Resources, European cyber security month (ECSM) (https://cybersecuritymonth.eu/press-campaign-toolbox)	ECSM resources available to be used with your campaigns and to support the ECSM initiative.	All threats	All roles
	Threat and Thematic Landscapes in interaction, ENISA (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes)	Published annual reports include thorough information about threats, attack vectors, i.e. schematic representations on the course of cyber-attacks.	All threats	All roles
	Diagnosing cyber threats for smart hospitals, ENISA (https://www.enisa.europa.eu/news/enisa-news/diagnosing-cyber-	ENISA presents a study that sets the scene on information security for the adoption of IoT in Hospitals. The study, which engaged information security officers from more than ten hospitals across the EU, depicts the smart hospital ICT ecosystem; and through a risk based approach focuses on relevant threats and vulnerabilities, analyses attack scenarios, and maps common	All threats	Management

	threats-for-smart-hospitals)	good practices.		
Risk Assessment & Checklists	How to handle health data	When health data relates to an identified or identifiable individual it is considered as personal data, and even a special category of personal data which requires additional protection. Therefore, certain processes and procedures have to be taken into account when handling health data.	GDPR violations	Access to clinical data
	How to handle personnel information	Healthcare organisations deal with a second category of data subjects, namely their staff. Therefore, certain processes and procedures have to be taken into account when handling personnel data.	Ransomware, Cyberespionage, Information leakage, Data breaches	Access to personal data
	How to detect a hacker	Every organisation that collects, processes, stores and transmits data is a potential target for cybercriminals. Healthcare organisations deal with valuable personal data, so it is not surprising that hackers try to obtain data from healthcare organisations.	All threats	IT
	Cyber incident response	Any organisation that works with digital technologies and deals with (sensitive) personal data should have an Incident response strategy in place. Some insights on incident response strategy.	All threats	IT and Management
	Assessing training needs	With the continuous risk and threat of cybersecurity incidents in healthcare, many organisations have implemented training programs to increase knowledge, skills and awareness of staff members. Training has been found to support both staff members in their tasks, prevent cybersecurity incidents from happening, as well as help to create a cybersecurity culture. Therefore, before implementing training	N.A.	Management

		programs, it should be clear what the actual specific training needs are so the best training program can be selected. This is often done through a Training Needs Assessment, or TNA.		
	How to establish a security culture	A large share of cybersecurity incidents in organisations have been attributed to the activities and behaviour of staff members. The culture within an organisation has a strong influence on staff behaviour and the choices they make in their work. Understanding the character of this culture is crucial information to both understand and improve how cybersecurity practices are integrated into healthcare organisations. As such, investing in a security positive culture will help to lower and prevent security incidents.	Inside threat, Data breaches, informatio n leakage.	All roles
	Risk management and assessment	Risk management is an essential process for any organisation, including healthcare organisations. While risk management is predominantly the responsibility of management level staff, the outcomes and decisions that follow the assessment affect the entire organisation. Cultures (within the organisation) can have a significant impact on the success of new cybersecurity measures.	All threats	Management
Case studies	AMCA Healthcare data breach case	A data security incident discovered in March 2019. Hackers gained access to AMCA's system and breached data included patient names, addresses, telephone numbers, dates of birth, dates of service, account Balances, banking or credit card information, and provider details.	Data breach	All roles
	Data breach on medical	A striking case occurred in	Data	All roles

	research	Great Britain, where hackers penetrated a protected system in 2 hours, attacking both the personal information of students and those of university professors, thus accessing the research databases.	breach	
	The ransomware in the healthcare sector	Basilicata Region in Italy was attacked by a powerful ransomware that irretrievably cancelled all documents on the computer and shared folders by sending emails without the possibility of retrieving them.	Ransomware	All roles
	The Wannacry cyber attack in the UK	The ransomware attack too many British health centres providing a devastating global cyber attack that crippled computers in hospitals across the UK and cost the NHS £92m.	Ransomware	All roles
	The Nansh0u campaign	A malicious global cryptojacking campaign infected 50,000 servers for months and took advantage of their great computing power, in order to undermine the open source virtual currency named TurtleCoin.	Cryptojacking	All roles
	Hackers attack Indian healthcare website	Hackers broke into a leading India-based healthcare website, stealing a huge amount of records containing patient and doctors' information and credentials. These cybercriminals are directly selling the data stolen in the underground markets.	Cyber espionage	All roles
	Malware-created cancer nodes	A simulated attack, developing a malware that can add realistic-looking but entirely fake diagnoses or hide real cancerous nodules that would be detected by the medical equipment.	Malware	All roles
	The Malware attacks to LifeBridge and Allied Physicians of Michiana	Two recently disclosed malware attacks in the healthcare sector illustrate that detection and mitigation of such attacks can be rapid, or it can take many months.	Malware	All roles

	Hospitals fined for GDPR violations	A GDPR violation has occurred in the Netherlands, where the authorities recently found a hospital in the Hague in connection with a data breach involving workers who inappropriately accessed the medical records of "a well-known Dutch person”.	GDPR violations	Management
	Phishing to patients’ emails to get bank accounts	multiple email accounts had been compromised between March 14 and April 3, 2018, and as is the case with most breaches of this kind, it stemmed from employees being tricked into handing over sensitive information via email	Phishing	All roles
	The first health care organization to be targeted by DDoS	Boston Children's Hospital became the first health care organization to be targeted by DDoS attacks from a hacktivist group. Because the hospital uses the same Internet Service Provider (ISP) as seven other area health care institutions, the organized DDoS attacks had the potential to bring down multiple pieces of Boston's critical health care infrastructure.	Denial of Service	Management and IT

4. Minimum quality standard

In order to provide a quality assurance report for future training actions in SecureHospital.eu project (e.g. workshops, webinars and summer school) a minimum quality standard has been developed. In particular, according to the quality points derived in deliverable **"D4.2 - Trainer interviews and workshop report (Public report)"**, the minimum quality standard has been defined, as shown in Figure 8.

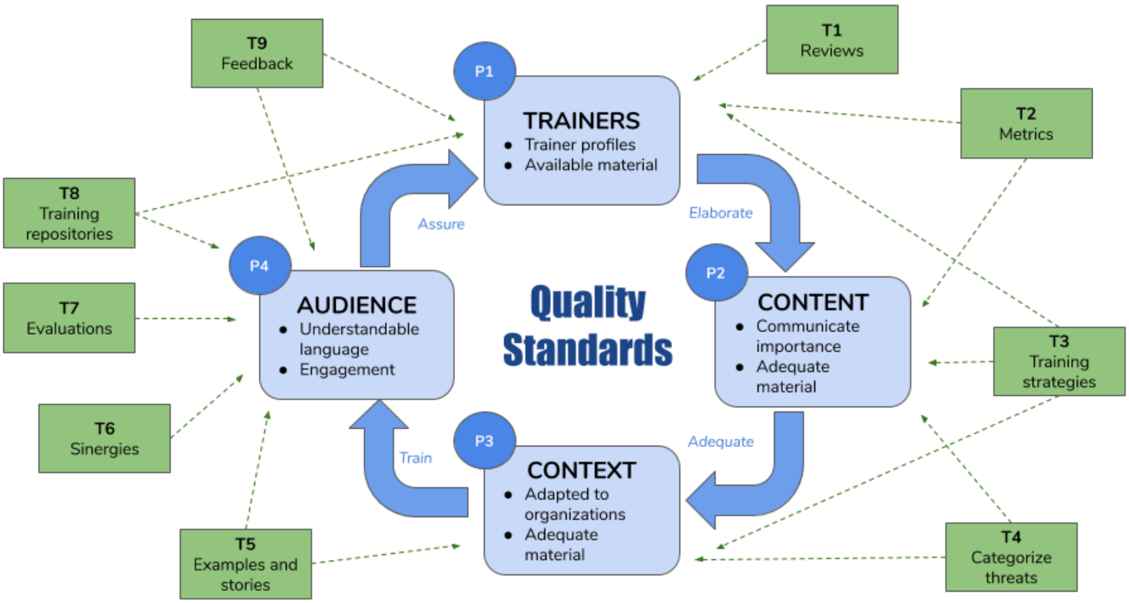


Figure 8. Minimum quality standard scheme

The minimum quality standard is based on four points (light blue squares), nine tools (green squares) in a continuous improvement approach (indicated with blue arrows).

In particular, the main points related to the relevant minimum quality standard have the following flow: P1) Trainers - Determine the materials and knowledge for the trainers assuming the risk of the training program, P2) Content - Decide the raw adequate material and according to the importance of communicating cybersecurity awareness, P3) Context - Check the training program fulfils the expectations and needs of the particular healthcare organization with adequate workable material and P4) Audience - Receive and respond to receivers expectation by utilizing a comprehensive language and sharing common experiences relevant to the training delivered.

In addition, potential tools/techniques to be used by the trainers are indicated and pinpointed for the specific quality standard point, which they apply to. Several tools are considered: T1) Reviews, T2) Metrics, T3) Training strategies, T4) Categorize threats, T5) Examples and stories, T6) Sinergies, T7) Evaluations, T8) Training repositories and T9) Feedback.

Finally, the minimum quality standard points are incorporated in a continuous improvement approach (indicated with blue arrows) while compiling the specific assurance report for each delivered training program.

5. Conclusions

This deliverable is an initial seed to start covering the identified gaps in literature & publications and training courses specifically directed to cybersecurity awareness raising in the healthcare sector. Among other deliverables related to SecureHospitals.eu, in particular D3.1, D3.3 and D4.1 allowed to identify the particular gaps in literature & publications, related projects and training programs.

As the scale and complexity of the cyber threat landscape is rapidly evolving, with increasing number of cyber-attacks on all types of organisations, the pressure on the cybersecurity resilience of organizations is also gaining importance. Organizations face a number of ICT security risks on a daily basis. To defend themselves against cyber threats, they need to leverage its people, processes and technology to protect organizational assets against threats via ICT. By investing in the people and their education, processes, and technology, organizations can become more resilient. Cybersecurity goes beyond the risk management process to be a shared responsibility of leadership, ICT staff, and other personnel. When properly taken care of, cybersecurity can be turned from risk to opportunity that improves patient health and business continuity of hospitals.

Most organizations have their own resources they can and shall utilize IT staff, infrastructure, databases, services and licenses they use, preventive measures they already have, etc. The framework shall aim the raising of cyber resilience by utilizing the existing capacities and infrastructure, pinpointing the strengths and weaknesses providing a clear development roadmap. Different departments and occupations require different level of understanding of the cyber domain and all of them require a solid foundation to build upon. The framework has to address capacity mapping, cyber resilience level measuring, utilizing available and mapping missing resources, adaptive learning technologies, dynamic content delivery and the capability to provide the constant recurring flow of the activities mentioned.

Training and educational framework and curriculum needs to address the topics of identification, protection, detection, response and recovery by a multilateral approach addressing all decision-making levels and departments. By addressing these topics, the state of reactive defence can be turned into proactive and managed defence as departments and employees will not just have a better cyber hygiene but also become aware of their and other's role, learn how to interact and communicate. Yet the framework and the curriculum have to be flexible, dynamic and customizable for the healthcare industry so organizations can apply them flexible to their own size, operations and capacity building strategies.

6. Next steps

All materials have been designed in the form of infographics and they will be disseminated widely across all available channels but primarily through the online hub.

Furthermore, it is recommended to keep generating up-to-date new material for Healthcare centres related to cybersecurity awareness raising. In particular, in short video formats as wells as images/infographics.

Based on this deliverable, also the upcoming iteration of the roadmap that leads trainers to the development of new curricula tailored to the needs for the training seekers (D4.4) will assess a detailed library of sub-sources ready to be implemented on the online hub and transfer the relevant knowledge to trainers.

7. References

Literature:

Security Awareness Program Special Interest Group PCI Security Standards Council, "Best practices for implementing a security awareness program", PCI Data Security Standard (PCI DSS) October 2014.

M. S. Jalali et al., "Cybersecurity in Hospitals: A Systematic, Organizational Perspective", J Med Internet Res, **20**, 2018.

J. Rajamaki, J. Nevmerzhitskaya, C. Virág, "Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)", IEEE Global Engineering Education Conference (EDUCON), 2018.

Ayala, L (2016) Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention. Fredericksburg, Virginia.

KPMG, (2016) HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities.

A. L. Bris, W. E. Asti, "State of cybersecurity & cyber threats in healthcare organizations: Applied Cybersecurity Strategy for Managers", Essec Business School, Harvard, 2017.

P. Jespersen et al., "Smart Hospitals: Security and Resilience for Smart Health Service Infrastructures", ENISA, Nov 2016.

"Review of Cyber Hygiene practices", ENISA, Dec 2016.

"Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity", ENISA, Dec 2018.

Websites:

https://lucysecurity.com/train-employees/, retrieved on 05.04.2019

https://www.kaspersky.es/enterprise-security/security-awareness, retrieved 05/04/2019.

https://www.rri-tools.eu, retrieved, on 16.04.2019

https://businessdegrees.uab.edu/blog/promoting-data-security-in-the-workplace/, retrieved on 17.04.2019

https://cybersecuritymonth.eu/, retrieved on 17.04.2019

https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf, retrieved on 26.04.2019

http://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-primer.pdf, retrieved on 03.05.2019

https://etl.enisa.europa.eu/#/, retrieved on 29.07.2019

Annex 1: Collected medical training programs curricula

Solution Name	Abstract	Curricula
Cybersecurity Awareness: Identifying Personally Identifiable Information	As we use our computers to play games, pay for goods and services, and apply for jobs, our online identity is constructed from bits of information that we may or may not be conscious of revealing or sharing. This course discusses different information sources about who we are, what we do, where we are, and with whom we are associated—and how we can protect that information from misuse or corruption. Instructor Jennifer Kurtz explains how personally identifiable information (PII) is formed, and how it is valued and used in the marketplace by legitimate and criminal actors. She also covers the formal and informal capture of PII; goes into the legal and regulatory properties of PII; dives into breach case studies in the medical, financial, educational, government, and commercial sectors; and offers PII protection practices for both individuals and organizations. This course was created and produced by Mentor Source, Inc. We are pleased to host this training in our library.	What is PII? Formal and informal capture Why is PII protected? Legal and regulatory influences High-profile PII breach cases: Medical, financial, and educational Global differences in PII use Protecting PII as an individual Best practices for organizations to protect PII
DoD mobile devices v1.1.	Cyber awareness challenge	In this presentation, Department of Defense (DoD) mobile device users will learn about significant security issues and vulnerabilities associated with unclassified mobile devices. The training begins by reminding DoD users that these devices are provided solely to support mission accomplishment and not for a user’s personal convenience. DoD users are cautioned that, as a user of a government-provided or government-authorized mobile device, they have responsibilities to help ensure the security of DoD devices. After reviewing the vulnerabilities of mobile devices and who is vulnerable, users are informed on how to protect against loss or theft, against compromise, and against malware. The training covers use of DoD mobile devices around classified information, as well as use of messaging services, use of wireless features, and other special considerations in DoD mobile device use. This training also defines removable storage media with associated vulnerabilities

		and limitations on use of removable media. Finally, DoD mobile device users are provided guidance on what to do if their DoD mobile device is lost, stolen, or compromised.
Phishing awareness v4	Cyber awareness challenge	This interactive training explains what phishing is and provides examples of the different types of phishing, to include spear phishing, targeting specific groups or individuals, and whaling, targeting senior officials. Phishing techniques such as deceptive e-mails and web sites, as well as browser "tab nabbing," are discussed. Guidelines are provided to help users to recognize phishing attempts, so that appropriate actions may be taken to avoid these attacks and their consequences. The training explains that phishing is a serious, high-tech scam and that system users are the best line of defense against phishing. Further, the training illustrates why users should always be on the lookout for phishing attempts, even from people from within their own organization.
Identifying and Safeguarding Personally Identifiable Information (PII) v3	Cyber awareness challenge	This training starts with an overview of Personally Identifiable Information (PII), and protected health information (PHI), a significant subset of PII, and the significance of each, as well as the laws and policy that govern the maintenance and protection of PII and PHI. The course is designed to prepare DoD and other Federal employees to recognize the importance of PII, to identify what PII is, and why it is important to protect PII. The Federal government requires the collection and maintenance of PII so as to govern efficiently. However, because PII is sensitive, the government must take care to protect PII, as the unauthorized release or abuse of PII could result in potentially grave repercussions for the individual whose PII has been compromised, as well as for the federal entity entrusted with safeguarding the PII. This course explains the responsibilities for safeguarding PII and PHI on both the organizational and individual levels, examines the authorized and unauthorized use and disclosure of PII and PHI, and the organizational and individual penalties for not complying with the policies governing PII and PHI maintenance and protection. This training is intended for DoD civilians, military members, and contractors using DoD information systems. This course may also be used by other Federal Agencies.

Security Awareness Training made simple	CFISA on-line courses makes it easy to Click and Train your employees. You can get started in minutes!	Level I Level I training provides an overview of the risk associated to cybercrime and best practices to protect the business from phishing, email threats and other cybercrimes. Level I Security Awareness Training 9 Lesson Course. Total Time: 58:53 Risk associated with cybercrime Creating strong passwords to increase security Understanding and recognizing social engineering Phishing and email best practices Protecting against viruses, spyware and spam Protecting your personal workspace Safe internet use Device management – Internet of Things Today's risks – acceptable use of electronic resources Level II Level II expands on Level I training and provides employees with a more robust cyber security awareness training experience. This course is designed to reduce company risk and enhances knowledge about protecting the workplace from identity fraud, how human behavior is exploited by cybercriminals and the business Impact of cybercrime. Level II Security Awareness Training 15 Lesson Course. Total Time: 111:36 Risk associated with cybercrime The impact of cybercrime and identity fraud Today's threats How behavior is exploited by cybercriminals Creating strong passwords to increase security Recognizing social engineering Phishing and email best practices Protecting against viruses, spyware and spam Protecting your personal workspace Security best practices away from the office Safe internet use Protecting the workplace from identity fraud Social Media Security Device management – Internet of Things Today's risks – acceptable use of electronic resources
Introduction to Cyber Security	To gain essential cyber security knowledge and skills, to help protect our digital life more and more depending on online services.	Threat landscape: terminology, cyber security threats, keeping up to date Authentication: access control, passwords, two-factor authentication Malware: types of malware, attack vectors, preventing infection Networking and communications: fundamentals, security challenges, standards

		Cryptography: symmetric and asymmetric cryptography, applications Network security: firewalls, virtual private networks, intrusion detection / prevention When your defences fail: cyber security laws, recovering from attacks Managing security risks: risk analysis and management
CapGemini	Collection of courses/workshops. See website link.	What is Cyber Security Awareness Cyber Security Awareness training aims to make the participants aware of the trends, challenges and needs around Cybersecurity. For consultants, this means providing a foundation to be a knowledgeable partner in the field of IT Security. For others, it enables them to understand what aspects of Cyber Security are relevant to perform their work safely. Also, the participants are made aware of the Cyber Security dilemmas that organizations face. After the training the participants will have: Insight into the trends, challenges and needs around Cyber Security. Insight into the worth of information. Understanding of why, when and where information security is applied. Insight into basic strategies and solutions for Cyber Security. Insight into the role played within the secure Cyber environment. Get acquainted with experts in the area of Cyber Security.
BeOne Development	Information security in healthcare: With the new awareness program, healthcare institutions and their employees learn to cope better with cyber threats and physical incidents. Anouk: "An example of a cyber threat that many companies face is phishing. How do you recognize fake e-mails and how should you deal with them? "Physical incidents also occur more often than you think. "Imagine that an employee leaves the medication list of clients somewhere unattended. With this, medical data can be inadvertently disclosed. In the new program we teach participants, among other things, how to prevent situations like this, "Anouk explains.	Cyber threats With the new awareness program, healthcare institutions and their employees learn to cope better with cyber threats and physical incidents. Anouk: 'An example of a cyber threat that many companies face is phishing. How do you recognize fake e-mails and how should you deal with them? ' Physical incidents also occur more often than you think. 'Imagine that an employee leaves the medication list of clients somewhere unattended. With this, medical data can be inadvertently disclosed. In the new program we teach participants, among other things, how to prevent situations like this', Anouk explains. Awareness The aim is to make employees aware of the threats and their own role in protecting themselves and their organization. "Awareness is a hugely important link in the process to change the behavior of employees, which ultimately makes them work safer and deal

		differently with privacy and information security in healthcare," Anouk says. The great thing about the program is that it appeals to a broad target group. 'It is not only intended for nursing staff, but also for office staff, cleaners and volunteers who work in healthcare. If you involve employees from all levels of the organization in the training, you will achieve the best results. "
Digital Health Compliance: Security Awareness Escape Room voor de zorg	The human factor is one of the most important factors in the field of cyber security. To protect a healthcare organization within the digital domain, it is necessary that all employees are aware of the risks that are present.	The human factor is one of the most important factors in the field of cyber security. To protect a healthcare organization within the digital domain, it is necessary that all employees are aware of the risks that are present. To optimally improve awareness, Deloitte has developed a learning experience in the form of an escape room game. This escape room is set up for a maximum of 5 to 6 healthcare professionals per round. The participants are challenged to solve 7 challenges within 20 minutes and thus complete the game. In the game, participants are asked to unlock a laptop that is infected with ransomware. All challenges in the game will test both knowledge and awareness of security among the participants. The challenges cover the following important security themes: Phishing emails Data classification Social Engineering Secure passwords Secure Wi-Fi use Safe handling of equipment Sharing data Dumpster diving
Digivaardig in de zorg	On this knowledge site you can work as a healthcare provider to improve your digital skills. Select the sector in which you work below and start today. The more digitally skilled you are, the more time you have for your client and the more pleasant you work.	The educational resources Basic skills Work on the basic skills that everyone needs to be able to work in healthcare. Information security & privacy Learn everything about handling information securely, online and offline. Technology & e-health Stay up-to-date on new developments such as gamification, big data and virtual reality. Apps & settings Learn to work conveniently and quickly with your (Android or iOS) phone or tablet. Office & 365

		Word and Excel are used everywhere. Here you learn to work with these important packages. Sharepoint, Teams and OneNote are also covered. Social media You can also use Facebook, Twitter, WhatsApp, YouTube and all other social media in your work. Care home automation In-house technology can make care for your client easier and better. Applications Every healthcare provider has to deal with different apps and systems. For example the ECD or Aysist.
Sincerus - eLearning	Awareness means continuous awareness of information security risks. Some risks can be limited with the help of technical measures. But most of the risks can be found in acting as part of human behavior. The E-learning method from Sincerus therefore focuses primarily on human actions. We give your employees insight into their own behavior. Because that largely determines the extent to which risk is run with regard to information security.	The target Awareness means continuous awareness of risks in the field of information security. Some risks can be limited with the help of technical measures. But most of the risks can be found in acting as part of human behavior. The E-learning method from Sincerus therefore focuses primarily on human actions. We give your employees insight into their own behavior. Because that largely determines the extent to which risk is run with regard to information security. Our approach We have developed our E-learning method as a complete awareness training. The method is made up of modules. Each module takes around 12 minutes in total. With animations, videos, practical examples and practical tips we teach your employees what their role is within the organization in the field of information security. And what their responsibilities are. As a result, they will work more safely and consciously. Do you want to make substantive adjustments or add custom modules to the training? We are also happy to help you with customized information security. The result The result of our E-learning is that employees are trained in a targeted manner and the previously determined information security level has been increased. By means of reporting you can easily gain insight into the knowledge of employees, your company in general or specifically per department. We conclude every

		E-learning process with an online knowledge test. And if the result is positive, the employee in question will receive a Security Awareness certificate.
Secura	The human factor plays an important role in the security of your IT structure. How well informed are your employees about information security and do they also act on this knowledge? To ensure that every employee in your organization becomes aware of IT security, Secura has developed the 'Security awareness' training course. In this short, lively training, your employees learn to understand the importance of proper data security and their own role in it.	The human factor plays an important role in the security of your IT structure. How well informed are your employees about information security and do they also act on this knowledge? With the help of social engineering , for example , cyber criminals can find out more about you and your company and take advantage of this, possibly without your knowledge. To ensure that every employee in your organization becomes aware of IT security, Secura offers an extensive set of Digital Security Courses, both basic courses and expert training. We offer our security awareness training under the name SAFE: Security Awareness For Everyone . With Training and Awareness you can strengthen the security culture of your organization in the basics. The focus is on the 'people ' aspect. Contact us without obligation to make an inventory of your needs and to arrive at a solution that seamlessly matches your question. Learn from the professional Secura has a solid track record in the field of training and awareness. We usually provide this service as in-house training, but we can also provide it for training and education organizations. The Secura experts are happy to share their knowledge with you. In practical workshops where you can take the role of a hacker or think of a security awareness training for your organization as a whole, for more security awareness in the workplace.