



## 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.



#### 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](http://www.google.com) and [www.google.com](http://www.google.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.



#### 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 designed to block access to a computer system until a sum of money is paid (e.g., prevent staff from accessing patient records or scheduling appointments).

### Search



### Learn



### Next Steps

Log on to [www.SecureHospitals.eu](http://www.SecureHospitals.eu) Online Hub





## 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.



## 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](http://www.google.com) and [www.gooogle.com](http://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.



### 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

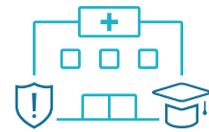
A zero-day threat is a threat that exploits an unknown computer security vulnerability. This means that there is no known security fix because developers are oblivious to the vulnerability or threat.



### 10. Ransomware

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid (e.g., prevent staff from accessing patient records or scheduling appointments).





## Cybersecurity Basics for Healthcare Organisations

### Share



#### 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.



#### Secure 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.

### Search



#### 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.

### Learn



#### 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 character, such as a punctuation mark.

### Next Steps

Log on to [www.SecureHospitals.eu](http://www.SecureHospitals.eu) Online Hub





# 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.



## Secure 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.



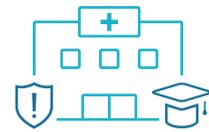
## Change Passwords Regularly

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.

Below are some examples of 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 character, such as a punctuation mark.





## Cyber Hygiene Basics

### Share



#### 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.

### Search



#### 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.

### Learn



#### Keep 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](http://www.SecureHospitals.eu) Online Hub





## 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:

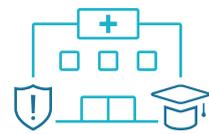
- System will not start normally.
- System crashes for no obvious reason.
- Internet browser directs you to unwanted web pages.
- Anti-virus software appears to be disabled.
- Many advertisements pop up on the screen.
- The user cannot control the mouse.



## Keep 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.





## How to promote a Cybersecurity culture in your organisation

### Share



#### 1. Raise Cybersecurity Awareness

- Education and training must be frequent and ongoing.
- Those who manage and direct the work of others must set a good example.



#### 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.

### Search



#### 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. Keep 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.

### Learn



#### 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.

### Next Steps

Log on to [www.SecureHospitals.eu](http://www.SecureHospitals.eu) Online Hub





### 1. Raise Cybersecurity Awareness

- Education and training must be frequent and ongoing.
- Those who manage and direct the work of others must set a good example.



### 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.



### Keep 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.



### 9. Be Prepared for Disaster

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



### 7. Secure Physical Access

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



### 10. Change Passwords Regularly

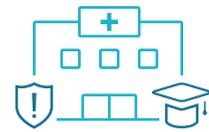
- Each staff member has a unique username and password.
- Passwords are changed routinely. Passwords are not re-used.



### 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.





## Common Cybersecurity Threats

### Entry Point



6 of the most relevant cybersecurity breaches' entry points in Healthcare...



PC

Mobile App.

USB Device

eMail

Comm. APP.

Network Access

Others

### Threat



9 of the most relevant cybersecurity threats in Healthcare and its common entry points...



Phishing



Cryptojacking



Ransomware



Spam



Malware



Cyberspionage



Identify theft



Information leakage



Inside threat

### Action - Promote Training:



**Spam:** to identify and safely erase. Also support to use new anti-spam software.  
**Phishing:** providing explanatory information.

**Inside threat:** explaining security policies.

**Identity theft:** to identify and providing procedures to keep identity protected.

**Ransomware:** providing explanatory information and raising awareness on safe documents.

**Cyberspionage:** keeping passwords secret, protecting screens and not leaving PCs unattended.

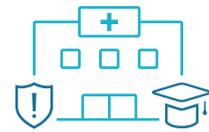
**Information leakage:** explain safe document deletion and destruction procedures.

**Cyrptojacking/Malware:** providing explanatory information and raising awareness.

### Cure

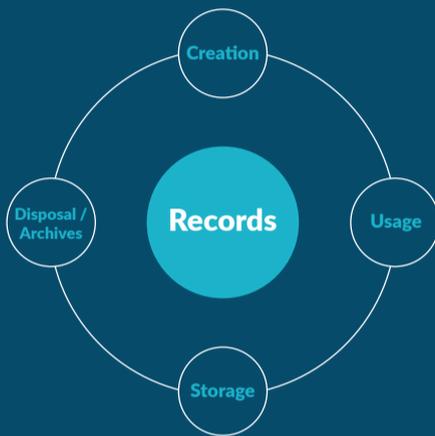
Log on to [www.SecureHospitals.eu](http://www.SecureHospitals.eu) Online Hub





# Connected Healthcare Centres 1/2

## Traditional



Traditionally, when patients arrive at the hospital they ask at the counter which office to go to. Once it's their turn, a nurse calls them by their name to enter the doctor's office.

The doctor checks the patients' health record on paper. In case of needing any additional test, the doctor fills out a receipt and it is delivered manually to the appropriate department. Once the department has the results, it delivers the results back to the doctor on paper again.

A couple of decades ago, with the advancement of technologies, this old procedure has been automated by integrating different information systems (Hospital Information System (HIS), Laboratory Information System (LIS), Picture Archive and Communication system (PACS)...).

## Smart

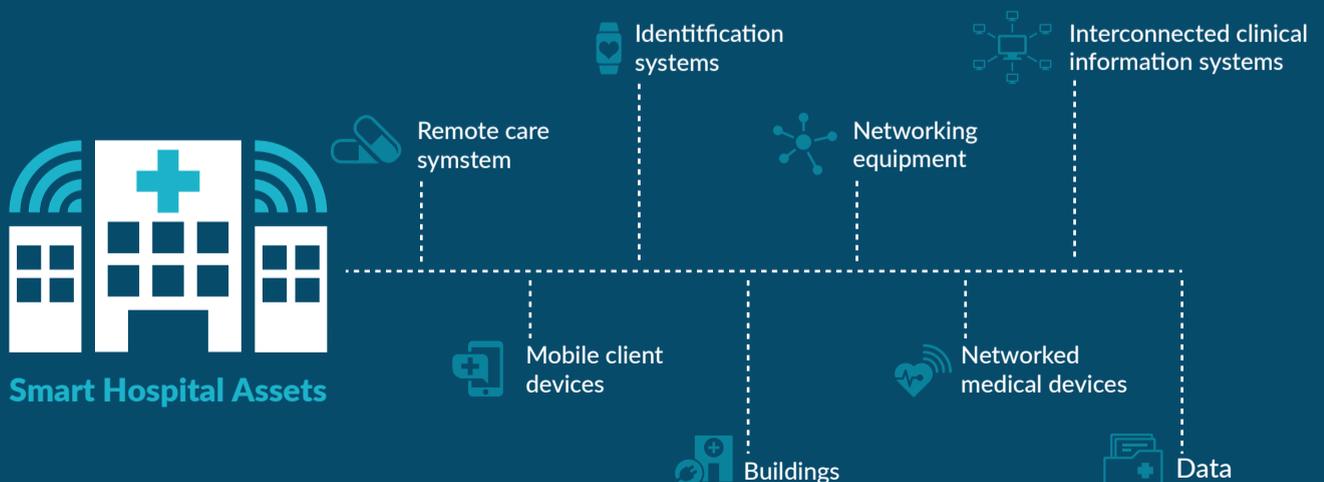


Nowadays, technology has allowed information to be shared between entities that were unthinkable a few years ago, exchanging information between different devices, sharing information between different systems and even crossing the barrier of hospitals to reach patients at home.

New communication channels between patients and hospitals have appeared, improving the quality of care, but also opening new cyber-attack surfaces to protect.

Depending on the professional role, it will have a different access level to the digital information in a hospital:

- **No access to patients' personal/clinical data** (e.g. staff in education, communication, finance, maintenance, human resources, research and innovation departments; mainly non-assistance staff)
- **Access to patients' personal data** (e.g. administrative staff)
- **Access to patients' clinical data** (e.g. medical staff)
- **Access to aggregated personal/clinical data** (Management team - CEO, CIO...)
- **Access to the source and all data** (IT department)





## Connected Healthcare Centres 2/2

### Trainings



To effectively incorporate security into existing quality assurance systems, training and guidelines are essential. Clear roles and responsibilities as well as regular training and awareness raising activities are key elements of a proactive approach to information security.

A training framework for the different staff roles is defined below

Complexity Level: ● Beginner ● Advanced ● Expert

#### Non-medical (no access to clinical nor personal patient's data)



- 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)
- Cryptojacking, ransomware, identity theft, data breaches / Plugins on browsers / Identify and complex credentials / Compliance to GDPR
- If interested same concepts as Management Expert

#### Medical (access to clinical and/or patient's data)



- 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)
- Cryptojacking, ransomware, identity theft, data breaches / Agents involved in cybersecurity / Plugins on browsers / Identify and complex credentials / Compliance to GDPR
- If interested same concepts as Management Expert

#### Management (access to aggregated clinical and patient's data)



- 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).
- 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 of handling data subject requests, how to make protection data impact assessment and who to involve)
- Denial of services / Insurances / Security policies / Access levels / Expertise in GDPR (real scenarios of handling data subject requests, how to make protection data impact assessment and who to involve)

#### IT (control of the database and access to all clinical and personal patient's data)



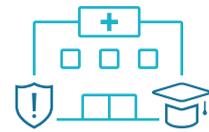
- Basic concepts of all threats and GDPR (technical measures required)
- Spam: anti-spam software / Denial of Services / Cryptojacking / ransomware / Information leakage / Creation of safe repositories / Firewall / Identify / Web traffic encryption / Configure browser / Identity management solutions / Audit and log user actions / Strong and complex credentials / Intermediate compliance to GDPR
- 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

### Cure



Log on to [www.SecureHospitals.eu](http://www.SecureHospitals.eu) Online Hub





### Raising Cybersecurity Awareness in Hospitals and Care Centres

#### Pain



**#1** According to ENISA, the **healthcare industry** jumped to the **top** in **cybersecurity attacks** in any industry

**+150 countries** and **+230,000 systems** across sectors and countries were **affected by cybercrime** on essential services connected to the internet, including **hospitals** and **ambulances**



**€** The medical sector has the **highest cost** for repairing the **cybersecurity** safety gap (375€ per medical health record)

According to CheckPoint.com, **cybersecurity** is still an **unresolved issue** of the medical sector, an environment where the **consequences** for patients can be **fatal**



**300%** increase in ransomware attacks since 2015



**€100b** global economy cost by serious cyber attacks

#### Research



The scale of the problem makes it necessary to act at the **European level**



More than **100 EU** research and innovation **programs** and initiatives aiming to improve cybersecurity

**25** national cybersecurity European agencies



**+1** strong European cybersecurity entities.

SECUREHOSPITALS.EU

**+200 literature and publication** items collected and analysed

**+100 cybersecurity programs** collected and categorized

**69%** of business have **no** or basic **understanding** of their exposure to cyber risk

**60%** of business have **never estimated** the potential **financial losses** from a major cyberattack

**51%** of European citizens feel not at all or **not well informed** about cyber threats

According to Kaspersky.com, **cybersecurity awareness raising programs** delivers proven results as

**90%** Reduction in the total number of incidents

**30x** Return of investment from purchase in security awareness programs

**86%** Participants willing to **recommend** the experience

**93%** Probability that knowledge will be applied in everyday work

#### Ecosystem



**+10 stakeholders groups**

**+28 national health systems or social security systems**

**>30 national cybersecurity agencies**

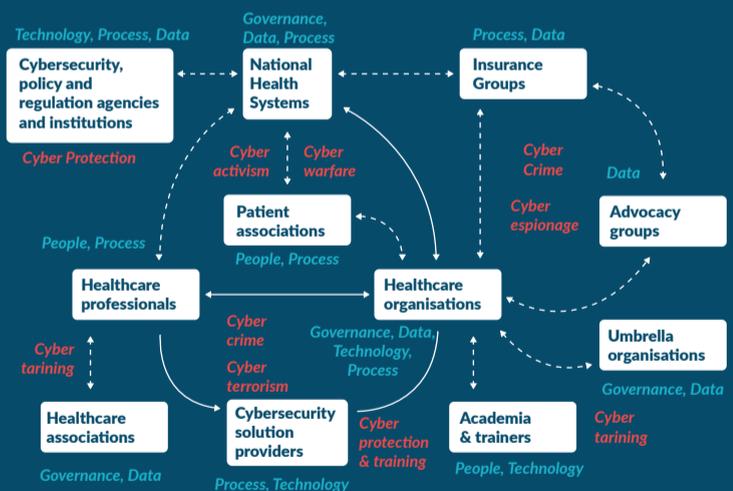
**>15,000 hospitals** and a vast number of care centres

**>10 million healthcare professionals**

**2,310 M€ European market**

**5 vulnerability types**

**5 attack motivations**



#### Cure



**Awareness raising** of staff working in healthcare settings on **security and data privacy**

**RAISE** awareness among decision makers and ICT practitioners in hospitals and care centres across Europe.

**AGGREGATE** all existing knowledge on cybersecurity in hospitals for the development of high quality and innovative trainings e-approaches.

**Training staff** working in healthcare settings

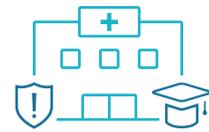
**CREATE** tailor-made training materials for trainers and IT practitioners to ensure the effective data protection, privacy and cybersecurity measures.

**COMMUNICATE** training needs, project training initiatives and further awareness raising on the online awareness and information hub.

**TRAIN** the trainers and practitioners all over Europe using different online and on-site methods.

**Proactive managerial and technological strategies to reduce vulnerabilities**





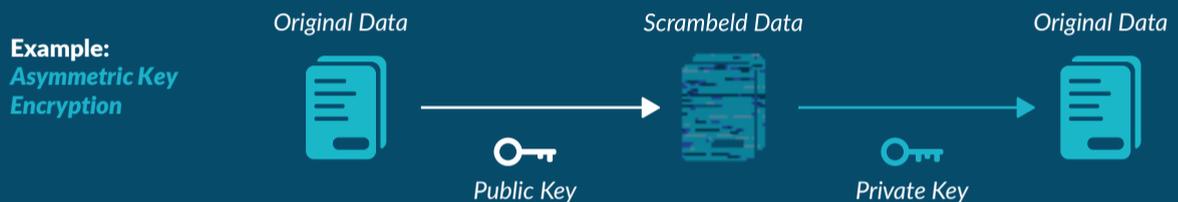
## Raising Cybersecurity Awareness - Encryption

### What is Encryption?



Encryption stands for a procedure to disguise the information in a way that it can travel along an insecure channel. Even if it is stolen, if the cyber-criminal does not have the key to decrypt it, the information itself is useless.

There are different encryption algorithms depending on the specific application to fulfill.



### Why is encryption important in healthcare?



Health data encryption occurs when data is converted into encoded and unreadable text in order to make the information inaccessible without a decryption key. Encryption helps protect patient health information when it's transmitted from one user to another.

#### How encryption works over networks?

HTTPS protocol ensures that the information travels secure. Transport Layer Security (TLS) is commonly used for encryption for transferring data securely over the HTTPS protocol.



When the protocol HTTPS is used, it is clearly shown in your browser as a closed lock.



### How



1. Your computer and the Server **agree** on how to encrypt.
2. Server **sends certificate**.
3. **Your computer** "starts encrypting".
4. **The server** "starts encrypting".
5. All messages are now **encrypted**.



### Cure



#### Awareness raising of staff working in healthcare settings on security and data privacy

**RAISE** awareness among decision makers and ICT practitioners in hospitals and care centres across Europe.

**AGGREGATE** all existing knowledge on cybersecurity in hospitals for the development of high quality and innovative trainings e-approaches.

#### Training staff working in healthcare settings

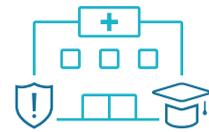
**CREATE** tailor-made training materials for trainers and IT practitioners to ensure the effective data protection, privacy and cybersecurity measures.

**COMMUNICATE** training needs, project training initiatives and further awareness raising on the online awareness and information hub.

**TRAIN** the trainers and practitioners all over Europe using different online and on-site methods.

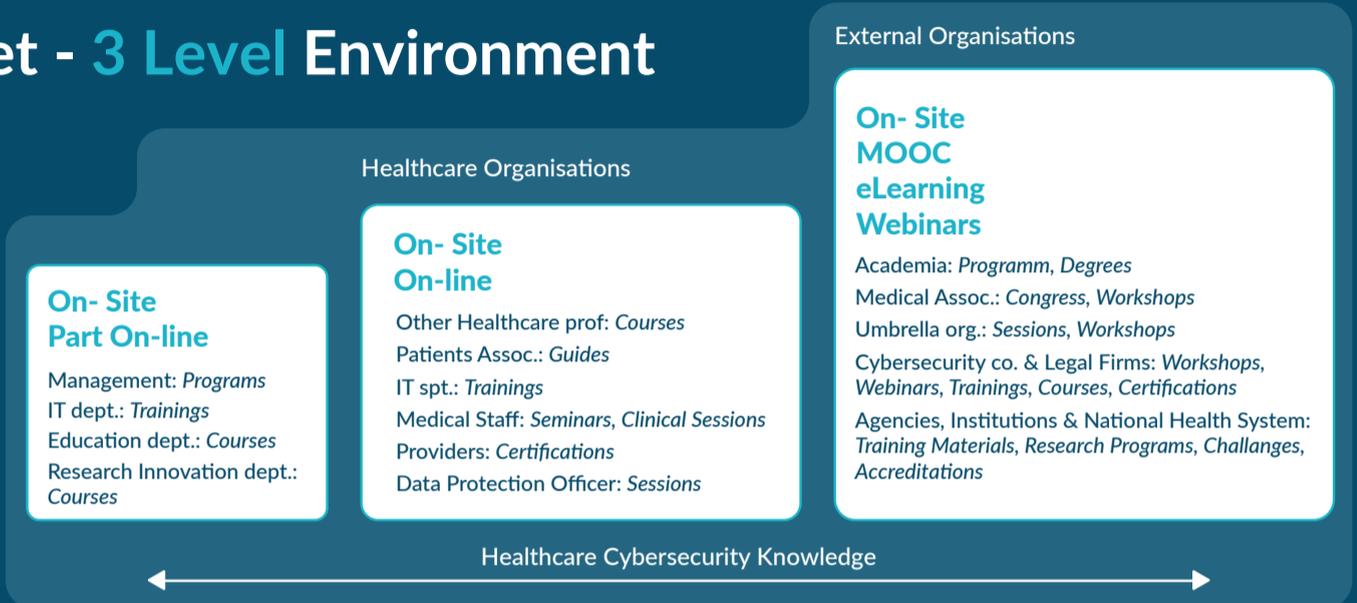
**Proactive managerial and technological strategies to reduce vulnerabilities**





# Raising Cybersecurity Awareness - Training Cybersecurity

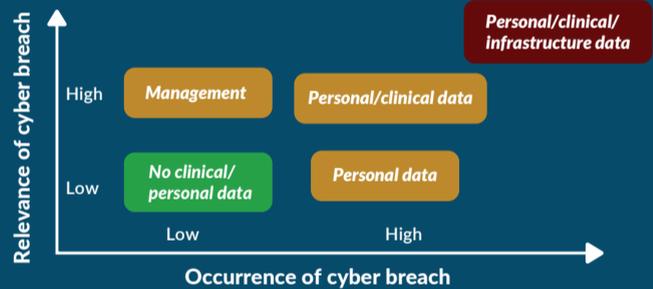
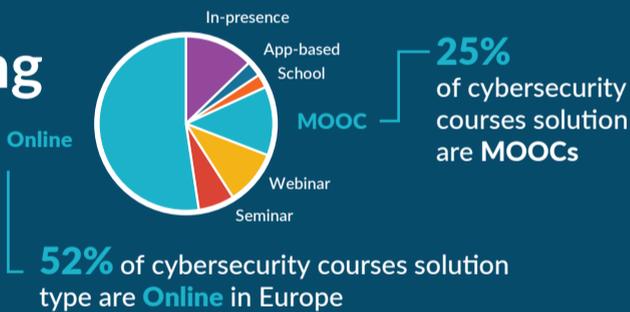
## Target - 3 Level Environment



**>7,3 million nurses**  
**>1,8 million physicians**  
EU European Commission ec.europa.eu | eurostat | statistics-explained  
**>10 Types of participant entities**

- Healthcare Organisation:** provide medical and health terminology and know-how
- External Organisations:** using this medical terminology, provide cybersecurity knowledge

## Training



Training allows the understanding by healthcare staff to manage technological terms

Different staff roles require specific training content

## Assessment

### Minimum quality standard

- 4 points (light blue squares)
- 10 tools (green squares)
- in a **continuous improvement** approach (indicated with white arrows)



## Cure

