Training materials for participants

The training was conducted by: 1+1 Spółdzielnia Socjalna

The training materials were created as part of the DISH DIGITAL & INNOVATION SKILLS HELIX IN HEALTH project. DISH is co-financed by the European Union Programme Erasmus+, Key Action 2 Cooperation for Innovation and Exchange of Good Practices – Sector Skills Alliances

Cybersecurity in healthcare institutions – 10 key issues

1. Create a safety culture
2. Protect mobile devices
3. Maintain good habits
4. Use a firewall
5. Install and update antivirus software
6. Expect the unexpected
7. Control access to sensitive data
8. Use strong passwords and change them regularly
9. Restrict network access
10. Control physical access

1. Create a safety culture

Security specialists agree: the weakest link in any computer system is its user.

Specialists in the field of psychology and sociology of information technology (IT) users prove time and again how difficult it is to raise people's awareness of cybersecurity. A key action was taken by IT system administrators and their users should be to reduce the likelihood that patients' personal health information will be exposed to unauthorized disclosure, modification, destruction, or denial of access. However, no action taken will be effective unless the healthcare practice is willing and/or able to apply it on an ongoing basis. It is crucial to enforce the information security policy and regular training for all users of the IT system so that they are sensitive to the importance of cybersecurity. In short, any health care practice must instill and support a safety-oriented organizational culture.

One of the most difficult aspects of ensuring cybersecurity is overcoming the belief that "this can't happen to me." People, regardless of their level of education or IT sophistication, believe that they will "never succumb to sloppy practices or compromise patient information. It only happens to other people."

It should be remembered that by following certain practices, you can avoid at least some mistakes resulting from overconfidence. It is the responsibility of every organization, including health care units, to support proper information security by establishing a safety culture. Every person in the organization must accept a common vision of information security so that habits and practices are automatic.

Security practices must be applied and not only written in documents regarding information security policy.

No checklist can adequately describe everything that needs to be done to establish an organization's safety culture, but there are some obvious steps to take:

1. Education and training in this field must be frequent and continuous.
2. Those who manage and direct the work of others must set a good example.
3. Taking responsibility for information security should be one of the core values of an organization.

The protection of patients through good information security practices should be carried out on an ongoing basis by the health service unit, in parallel with all activities involving taking care of the health of patients.

2. Protect mobile devices

Mobile devices – laptops, tablets, smartphones, portable storage media have greatly facilitated information management, also in healthcare. At the same time, however, they have created a catalog of completely new threats to privacy and information security. Some of these threats overlap with those specific to desktops, but some are unique and we will focus on them at this point.

In the case of mobile devices, we must pay attention to the fact that:

1. Due to their mobility, these devices are easy to lose and prone to theft.
2. Mobile devices are more vulnerable to electromagnetic interference than desktop computers. This applies to m.in interference generated by other medical devices. These interferences can, in extreme cases, damage data stored on mobile devices.
3. Since mobile devices can be used in places where they can be seen by others, the user must take special care to prevent unauthorized suspicion of health information displayed on a laptop, for example.
4. Not all mobile devices are equipped with strong authentication and access control. Additional steps may be needed to protect mobile devices from unauthorized use. Laptops, mobile phones, tablets should at least be password protected. If password protection is not provided, additional steps should be taken to protect electronic health information on the mobile device, including additional precautions regarding the physical control of the device.
5. Laptops and mobile devices are often used to wirelessly transmit and receive data. This wireless communication must be protected from eavesdropping and interception. Cybersecurity experts recommend not to transmit electronic health information on unencrypted public networks (e.g. public wifi networks, especially those that are not password protected).

Transferring data using mobile devices is inherently risky. Therefore, the use of mobile devices should be particularly justified by the higher necessity in this respect. The argument about greater convenience/comfort of work is not enough in this case.

Where it is necessary to send electronic health information to or from a mobile device, cybersecurity experts recommend encrypting the data. Do not use mobile devices that do not support this encryption.

If it is necessary to take a laptop containing electronic health information out of a healthcare facility, you should secure the information on your laptop's hard drive with encryption.

The rules that define the circumstances in which equipment can be removed from the facility are very important and special care should be taken when developing and enforcing these rules. The primary goal is to protect the patient's information, so considerations of convenience or practice (e.g. working from home) must be taken into account in this regard.

Remote work, m.in due to the COVID-19 pandemic, has become extremely popular. Those responsible for protecting patient information must realize that their responsibility does not end at the office door. Good privacy and security practices should always be followed.

3. Maintain good habits

The doctor knows the importance of healthy habits for maintaining good health and reducing the risk of infections and diseases. The same applies to information systems. For them to work properly and reliably, proper prevention is needed. This is particularly important in a situation where these IT systems store sensitive data about patients. In this respect, we can observe a very clear analogy concerning health prevention – sometimes very small things can be crucial.

Properly configure your computer software

New computers and software packages often have a staggering array of capabilities. At the same time, however, hardware/software vendors very often skimp on how to properly configure them to keep the system secure. Faced with this complexity, it may be difficult for a standard user to decide which options to allow and which to disable. However, there are several relatively universal rules in this regard:

1. Uninstall any apps that aren't necessary to run a healthcare facility (e.g., games, instant messaging, photo sharing tools). If the purpose of the application is not obvious, check the software manufacturer's website to learn more about the purposes and uses of the application. If you have doubts about the importance of a particular application, please contact your system administrator.
2. When installing the software, do not accept the default or "standard" settings. Review each option, review possible choices, and contact support if necessary.
3. Find out if the vendor of your medical unit application is extending an open connection to the installed software ("back door") to provide updates and support. If so, provide a secure connection at the firewall and ask them to disable this access when not in use.
1. Disable remote file sharing and remote printing as part of the operating system configuration. Allowing this may result in files being accidentally shared or printed in places where unauthorized persons can access them.

Software Update

Most software needs to be updated periodically to ensure security and introduce additional features. Providers can send updates in a variety of ways: automatic downloads or downloads at the user's request.

Updating the software is critical to maintaining system security because many of these updates address newly discovered vulnerabilities in the product. In larger enterprises, such "patching" can be a regular, everyday task (if we use many applications, it may turn out that almost every day which of the providers has prepared a new update). We may not have enough resources in the unit to constantly monitor new updates and install them at the right time. Therefore, it is worth setting up automatic updates wherever possible (e.g. use Microsoft Windows automatic update). Regardless, at least one employee should monitor the information provided by the key manufacturers of the

software used by the facility on an ongoing basis (especially in the case of patient data management applications). When any critical patches appear, care should be taken to ensure that they are installed as soon as possible.

Operating System Maintenance (OS)

The operating system tends to accumulate outdated information and settings unless regular maintenance is performed. Thus, you should regularly monitor all computers, and if possible, regularly format the hard disks and install the operating system from scratch.

We should regularly check m.in.:

1. Whether the accounts of former employees are properly and timely disabled. In the event of dismissal of an employee on the initiative of the employer, access to the account should be blocked before the notice is served.
2. Computers and any other devices, such as photocopiers, on which data is stored are properly cleaned before disposal. Even if all the data on your hard drive has been deleted, it can still be recovered using commonly available tools.
3. Old databases and files with personal data are archived under appropriate conditions or completely deleted from the system if they are no longer needed, under the applicable data processing requirements.
4. Software that is no longer needed is fully uninstalled (including test software and old versions of the current software).

How do you know if staff members have downloaded programs they shouldn't?

Many commercial applications and services can be configured to report or even stop the download of unauthorized software. We may also use applications to perform vulnerability and configuration analysis, and some applications/services may also perform general security audits.

4. Use a firewall

Every healthcare facility that uses the Internet (i.e. at the moment EVERY facility) should have a properly configured firewall. This firewall protects your local area network (LAN) from intrusions and threats from external sources. While antivirus software will help find and destroy malware that has already emerged, the firewall's job is primarily to prevent intruders from entering. In short, an antivirus can be thought of as infection control, while a firewall is designed to prevent disease.

A firewall can be both an appropriate application installed on a server computer and a dedicated device connected at the router/access point. In both cases, its task is to check all data coming to the system from the outside (from the Internet or a local network) and decide, according to predetermined criteria, whether this data should be passed.

Installing and properly setting firewall parameters can be technically complex, and hardware firewalls should be configured by trained technical personnel. Software firewalls, on the other hand, are often preconfigured with common settings that work in many standard situations. Software firewalls are included with some popular operating systems, protecting at the installation stage (such a basic firewall has, for example, MS Windows). Alternatively, separate Firewall software is widely available from computer security providers, including most antivirus software providers. These providers usually provide technical support and guidance on how to install a firewall so that people without more advanced technical knowledge can handle it.

When should I use a hardware firewall?

For large companies that use a local area network (LAN), consider a hardware firewall. A hardware firewall is located between the LAN and the Internet, providing centralized management of firewall settings. This increases LAN security by ensuring that the firewall settings are identical for all users of the local network.

However, it should be remembered that if the hardware firewall is to fulfill its role, it should be configured regularly monitored, and maintained by a specialist in this field.

5. Install and update antivirus software

The basic tool for attacking INFORMATION systems (especially in a small office) are computer viruses, which exploit vulnerabilities in the computer. These vulnerabilities are ubiquitous due to the nature of the computing environment. Even a computer that has all the latest security updates for the operating system and applications can still be at risk due to previously undetected errors. Computers can be infected by seemingly innocent external sources, such as CDs, e-mail, USB flash drives, or files downloaded from the network. Therefore, it is important to use a product that provides constantly updated protection. Antivirus software is widely available, well tested for reliability, and costs relatively little.

Your antivirus software must be up to date. Antivirus products require regular updates from the vendor to protect against the latest computer viruses and malware. Most antivirus programs automatically generate reminders about these updates, and many can be configured to allow automatic updates.

Without antivirus software, data can be stolen, modified, or destroyed, and attackers can take control of your computer.

How can users recognize a computer virus infection?

Some common symptoms of an infected computer are:

1. The system does not start normally (e.g. "blue screen of death")
2. The system freezes repeatedly for no apparent reason
3. The web browser opens unwanted websites
4. Antivirus software not working
5. Many unwanted ads appear on the screen
6. User cannot control mouse/pointer

6. Expect the unexpected

Sooner or later, something unexpected will happen. This statement at first glance seems like a cliché, but it is unfortunately true. Fire, flood, hurricane, earthquake, and other natural or man-made disasters can strike at any time. Important medical records and other key assets must be protected from loss as a result of these events. Therefore, we must take care of two key things: regular data backups and a well-thought-out backup plan, i.e. recovery of lost data.

In the business world, backup is a constant practice. However, in practice, staff members may be only familiar with the home computing environment, in which backup is rarely considered, at least until a failure occurs (and then it is very often already too late to apply any countermeasures). In a professional environment, you should create regular and reliable backups. A reliable backup is one you can count on in an emergency, so it's important not only to save all your data correctly but also to restore it quickly and accurately. Backup media should be tested regularly for their ability to restore properly.

Regardless of the media used for the backup, it must be stored securely so that the dish cannot be damaged by the same failure that happened to the main system. A good solution is to back up to remote servers. The solution may also be the use of the data cloud to create backup copies. Such a solution is cheaper than physical infrastructure, but you need to choose an operator of this type of solution with great caution.

Critical files can be manually copied to backup media, although this is a tedious solution and potentially prone to errors. If possible, use an automated backup method.

Some types of backup media, such as magnetic tape or removable hard drives, are reusable. It must be remembered that they can wear out over time, so you need to regularly monitor their condition.

Restoring data from a backup should be based on a clear and prepared procedure. This is important because, in the event of any disaster, patients' medical data should be restored as soon as possible.

A fireproof, permanently installed home safe, the combination of which is known only to a healthcare professional, maybe the best choice for many small health centers to store backup media. This does not place a backup outside the danger zone of a general disaster (earthquake, hurricane, nuclear weapons), but provides at least some protection against local emergencies such as fire and flood. Fireproof portable boxes or safes are by no means an insufficient solution.

7. Control access to sensitive data

A key element of building an IT system resistant to cyber attacks is regular password hygiene (indicated in point 8). However, a password is only half of what makes up a user's credentials. The other half is a login or username. In most computer systems, these credentials (login and password) are used as part of an access control system in which users are assigned specific data access rights. This access control system can be part of an operating system (e.g. Windows) or built into a specific application (e.g. e-prescription module). The ADMINISTRATOR of the IT system should limit access to data in such a way that each user obtains only the information that is necessary for him/ her work – not everyone needs to know everything!

In small units, you can restrict access to files/databases manually by using an access control list. This can only be done by someone with administrative privileges to the system. Before you set these permissions, it's important to determine which files should be available to which staff members.

Additional access controls that can be configured include role-based access control, in which the role of a staff member in the clinic (e.g., physician, nurse, billing specialist) determines what information can be accessed. In this case, make sure that you assign staff to the appropriate roles, and then set the access permissions for each role correctly, taking into account the needs of the position.

What happens if someone without permission has access to electronic health information?

In certain circumstances, such an incident is considered a violation that must be reported to the President of the Office for Personal Data Protection. Having good access controls and knowing who viewed or used the information (so-called access log) can help prevent or detect such violations.

8. Use strong passwords and change them regularly

Passwords are the first line of defense in preventing unauthorized access to any computer. Regardless of the type or operating system, a password should be required to log in. While a strong password won't stop attackers from trying to gain access, it can slow them down and discourage them. In addition, strong passwords combined with effective access control help prevent accidental abuse (e.g. they can curb employees' curiosity about a matter about which they should not have complete information).

Strong passwords are primarily those that are difficult to guess. Attackers can use the so-called dictionary breakers, which will check the combinations of the most frequently appearing phrases based on prepared dictionaries.

Strong passwords should not contain:

1. Words found in the dictionary, even if they are slightly changed (e.g. replacing a letter with a number)
2. Personal data, such as date of birth, names (own or family members or pets), PESEL numbers. Remember: If there is any information about you on a social network, it should never be used in the password.

Below are some examples of the characteristics of strong passwords:

3. Length of at least eight characters (the longer the better)
4. Combination of uppercase and lowercase letters, one number, and at least one special character, such as punctuation

Finally, systems should be configured so that passwords are changed regularly. While this can be inconvenient for users, it also reduces the risk of easily hacking into the system using a stolen password.

Passwords and strong authentication

Strong or multi-factor authentication combines many different authentication methods, which provides very high protection. In addition to the username and password, another authentication method is used (e.g. smart card, keychain, fingerprint, or iris scan).

What about forgotten passwords?

Anyone can forget the password, especially if it is long. To discourage people from saving passwords and leaving them in unsecured locations, create an opportunity to reset passwords relatively simply.

Examples of solutions:

1. Authorize two different staff members to reset passwords
2. Creating/making available within the IT system the function of resetting passwords

9. Restrict network access

Due to their ease of use and flexibility, modern network tools are very attractive. Web 2.0 technologies, such as peer-to-peer file sharing and instant messaging, are popular and widely used. Wireless routing is a quick and easy way to set up a broadband connection for your home or office. However, due to the confidentiality of healthcare information and the fact that it is protected by law, tools that can enable bystanders to gain access to a healthcare facility's network must be used with extreme caution.

Wireless routers are widely used at the moment, both by small and larger entities. If the wi-fi on the wireless router is not secured, its signal can be received from a distance, including, for example, from the parking lot of the building, other offices in the same building, and even nearby houses. Since electronic health information transmitted over a wireless network must be protected by law, it is important to secure the wireless signal so that only those who have access to the information can receive it. Wireless routers must be configured to operate only in encrypted mode.

Patients' mobile devices should not be able to automatically connect to a wifi network without providing a password. Setting up a network for secure guest access is costly and time-consuming, so the best defense is to prohibit accidental access. When a wireless network is configured, each corporate device should be identified on the router, and only then should access to the network be guaranteed for it.

Applications that use a peer-to-peer model (m.in for file sharing and instant messaging) can expose connected devices, including allowing unauthorized access to the devices on which they are installed. Verify that peer-to-peer applications have not been installed without authorization. It is not enough to simply disable these programs or uninstall them. A machine containing peer-to-peer applications can contain code snippets that can be used even after the programs have been removed.

A good rule of thumb is to prohibit staff from installing software without prior permission.

10. Control physical access

It's not just resources like files and data that need to be secured. The devices that make up the IT system themselves must also be adequately protected against unauthorized access. The most common way electronic health information is at risk is through the loss of devices, whether it is accidentally or as a result of theft. Incidents reported to the President of the Office for Personal Data Protection show that more than half of the cases of data loss are related to lost devices, especially portable ones (e.g. USB flash drive, tablets, laptops). However, there are also thefts of desktop computers, but even sometimes the hard drives themselves are torn out of the machines.

If the data storage device disappears (no matter how well the institution has taken care of the appropriate passwords, access controls, and file permissions), there is a possibility that a specific person will gain access to the data on it. That's why it's important to reduce the risk of your devices being lost or stolen.

Physical security of devices and data should focus on physical access limitations, e.g. securing devices in enclosed spaces/armored cabinets, managing access to physical keys, or restricting the ability to remove devices from a secure area.

Where should I place the server that stores electronic health information?

When considering the location of a server containing electronic health information, two main factors should be taken into account: physical protection and environmental protection. Physical protection should focus on preventing unauthorized access to the server (e.g. storing the server in a closed room accessible only to staff). Environmental protection should focus on protecting the server from fire, water, and other harmful factors (e.g. do not create a server room in a room located just below the toilet, if possible the server should not be located in a room with windows, and the right temperature and air circulation should be ensured).