elfh

elearning for healthcare

DATA SECURITY AWARENESS

VOLUNTEER INDUCTION

DATA SECURITY AWARENESS

We all have a duty to protect people's personal information in a safe and secure manner and share appropriately.

Everyone should be able to trust that their personal information is protected.

A person's safety is supported when the confidentiality of personal information is maintained, its integrity is protected against loss or damage and the information is accessible by those who are authorised.

Organisations must ensure that information is used appropriately and only when absolutely necessary.

THE VALUE OF INFORMATION

It is important to comply with the law to protect personal information. Poor security can cause personal, social and reputational damage.

Losing Information

Personal information may not be protected if:

- **Computers or mobile devices are lost**
- **Information is disclosed over the phone**
- **Faxed paper records are lost or sent to the wrong place**
- **Paper records are left on photocopiers or printers**
- **Theft of information**
- **Insecure storage**

Theft of Information	Information can easily be stolen by criminals, for example, if you click a link to a fake website.
Insecure Storage	If your paper or computer records are insecure, or if they are not disposed of securely, they can easily be lost or stolen.

DATA SECURITY AWARENESS

When volunteering you will come into contact with various types of personal and sensitive information. It is important to be able to identify these different types of information so that they can be appropriately protected when they are used and shared.

PERSONAL INFORMATION

Information about someone is 'personal' when it identifies an individual. Eg Name and Address

ANONYMISED INFORMATION

Anonymised information does not identify a person, so it cannot be personal or confidential.

CONFIDENTIAL INFORMATION

Confidential information can include names and addresses, as well as a person's sensitive personal information, for example, health and care information.

PSEUDONYMISED INFORMATION

Pseudonymised information is information in which individuals are distinguished by using a unique identifier, that is, a pseudonym.

This does not reveal their real identity but allows the linking of different data sets for the individual concerned.

INTRODUCTION TO LAW

Rights – Everyone has the right to:

- Make requests to access their own personal information. This is known as subject access requests (SAR)
- Have inaccuracies corrected
- Have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances
- Object to direct marketing
- Restrict the processing of their information, including by automated decision-making systems or programmes

Recording facts

- In addition to accurately recording facts, we must consider that the individual might be able to view their record online.

Access

- When providing people with access, care must be taken not to reveal information that they do not already know relating to third parties.
- For example, information in their record about family members, other service users and so on.

GDPR

GDPR is a set of rules governing the privacy and security of personal data and information

As a volunteer, if you do process personal data, then you must:

- Know the purpose of needing the individual's data
- Be transparent
- Only collect the personal data you need

For further information, or if you think this relates to your volunteer role, then ask your volunteer coordinator.

Freedom of Information Act

Where an organisation uses public money, the Freedom of Information Act 2000 puts a duty on the organisation to provide information to individuals who make a written request for it. Members of the public can make Freedom of Information (FOI) requests in three ways – by letter, fax or email.

Handling Freedom of Information requests is a technical skill that should be dealt with by trained staff.

As a volunteer you will not be expected to handle Freedom of Information requests. If you come across a FOI request, speak to your volunteer coordinator in the first instance who will be able to advise you accordingly

GOOD RECORD KEEPING

In some roles you may be required to create and update records in your organisation. These records should be:

- Recorded as the event occurs
- Complete
- Free from duplication
- Quick and easy to locate
- Compliant with procedures

It is important that records are full, accurate, dated and timed. They should distinguish between service user records, your opinions and any information provided by others.

- Be accurate
- Record information while the event is still fresh in your mind
- Enter accurate information into records and ensure that the information is kept up to date
- Give individuals the opportunity to check and confirm the details held about them
- Avoid creating duplicate records

THREATS TO DATA SECURITY

Criminals will often take weeks and months getting to know a place before even coming through the door or making a phone call. There are examples of many people being scammed by criminals pretending to be calling from a call centre.

For example, they may say they are calling about an online order you've made. If you're expecting a delivery, it is easy to be taken in.

The criminal may already have a lot of information about you and ask you to confirm additional details about your online account, so that the order is not delayed.

If they have your email address, they may try to get you to click on a malicious link in an email they send you.

ON THE PHONE
A criminal might call and pretend to be from your organisation, or a trusted outside authority, such as the police or an auditor.

IN THE OFFICE
'Can you hold the door for me? I don't have my key/access card on me.'
How often have you heard that in your building? Although the person asking may not seem suspicious, this is a very common tactic used by criminals.

PREPARATION
Their preparation might include finding your organisation's details online.

The goal is always to gain the trust of one or more colleagues, through a variety of means.

ONLINE
Social networking sites have opened a whole new door for scams.

One of the latest scams involves the criminal posing as a Facebook 'friend', however, you can never be certain that the individual you are talking to on Facebook is a real person.

Criminals are stealing passwords, hacking accounts and posing as friends for financial gain.

SOCIAL MEDIA

Revealing any information about your organisation on social media can be valuable to a criminal.

What information could a criminal get?

- Find out where John's office is by searching his organisation's website, then aligning John's online pictures to that office
- Gain access to John's office using the door entry code

What could a criminal do with this information?

- Install malicious software that corrupts data or prevents the organisation using it until they pay a ransom
- Gain access to data to sell on to other criminals
- Access details listed in the system, to steal a person's details

Look at the messages on the mobile phone. A criminal reading these posts will gain vital intelligence about how the organisation's processes work.

elfh
elearning for healthcare

EMAIL

Email can be the most efficient option for exchanging information securely but, as with all forms of information transfer, there are risks.

Hackers and criminals sometimes use uninvited emails that contain attachments or links to try to trick people into providing access to information. This type of threat is known as 'phishing'.

Remain vigilant and report the suspicious emails to your volunteer coordinator.

Never give your login details to anyone.

GOOD PRACTICE

It is important to use strong passwords on all of your devices to prevent unauthorised access. You should also use different passwords for each account.

There are some simple steps that you can take to increase the physical security of your organization:

- Do query the status of strangers (if it is safe to do so) especially if they try to follow people into restricted areas.
- Do shut or lock doors and cabinets as you are required
- Do wear your building pass or ID if issued
- Do maintain a clear desk policy when away from your desk
- Do know who to tell if anything suspicious or worrying is noted.
- Don’t tell unauthorised personnel how the security or other business-sensitive systems work.
- Do know what an incident or breach is in your organisation and know when and how to report one.

DATA BREACHES

The most common forms of security breaches are:

- Loss or theft of paperwork
- Data posted or faxed to the wrong recipient
- Emails sent to the wrong recipient
- Personal details mistakenly given over the phone

TELEPHONE

If a request for information is made by phone, you should, where possible, adhere to the following processes and procedures:

- Confirm the name, job title, department and organisation of the person requesting the information
- Confirm that the reason for the information request is appropriate
- Take a contact telephone number. For example, the main switchboard number – never a direct line or mobile phone number so that you can phone back and confirm that the caller is genuine
- Check whether the information can be provided – if in doubt, tell the person you will call them back
- Only provide the information to the person who requested it. Do not leave messages
- If in doubt, check with your volunteer coordinator first

ACCESS TO BUILDINGS

Last week, someone in a high-visibility vest visited a social care office in the local area. He followed a member of staff into the building and told the receptionist that he needed everyone's details for a 'software update'.

The person then sold these details to other criminals. Let's find out what else he was able to do.

Doors
Nearly every door the intruder encounters is open. Even those doors marked as 'restricted access' have been propped open to allow for a delivery.

This means he is able to wander in and out freely without challenge and could have stolen equipment or personal items belonging to staff.

Visitors
The intruder has forged a badge. He approaches the reception desk and asks for directions to the server room. They are happy to help. His badge isn't even checked. With access to the server room, he can disrupt the server as much as he likes, causing connectivity problems across the whole organisation.

Desks
Despite most organisations having strict clear desk policies, it is amazing how much data is found in unoccupied office areas. Financial documents, including client account details, are lying on desks.

The intruder has a bag of memory sticks and randomly disperses them on desks in the hope that someone will plug one in. It will then start installing malicious software onto the computer.

KEY POINTS

- We all have a duty to protect public information in a safe and secure manner
- We all have a responsibility to use information lawfully
- Make sure that information is shared in a secure way and that you have consent to do so. Give individuals an opportunity to check the accuracy of information and records held to enable any mistakes to be corrected
- By following good practice, you can help to ensure that personal information is not put at risk
- Good data security is important and we are all bound by legal requirements

elfh

elearning for healthcare

THANK YOU!

The content of this training was developed by NHS England, E-Learning for Healthcare and has been adapted by **Bradford Teaching Hospitals NHS Foundation Trust**, to provide an accessible format, ensuring that all volunteers have the same basic learning when they start in their role.