Data Security Awareness Level 1 Workbook

Name:

Job role:

Department:

Contents

Data Security Awareness - Level 1 Workbook

Welcome

NHS Digital delivers information and technology for better health and care.

We have developed this workbook to:

- Help health and care staff use and share information in a lawful and secure way.
- Promote good practice that should be adapted for your working environment.

Description

Your organisation is required to provide annual training on topics such as:

- The Data Protection Act 1998.
- The Freedom of Information Act 2000.
- The adoption of technology – building and maintaining public trust in how we use and share information.
- Information security policy and procedure.

This workbook provides an overview and guidance and good practice on the above topics.

Author: NHS Digital (Data Security Centre and External IG Delivery)

Duration: Approx. 1 hour

Learning objectives

By the end of this workbook you will understand:

- The principles and terminology of information governance (IG).
- Basic data security / cyber security terminology.
- The importance of data security to patient/service user care.
- That law and national guidance requires personal information to be protected.

And be able to:

- Explain your responsibilities when using personal information.
- Identify some of the most common data security risks and their impact.
- Identify near misses and incidents and know what to report.
- Distinguish between good and poor practice when using personal information.
- Apply good practice in the workplace.

Why is data security important in health and care?

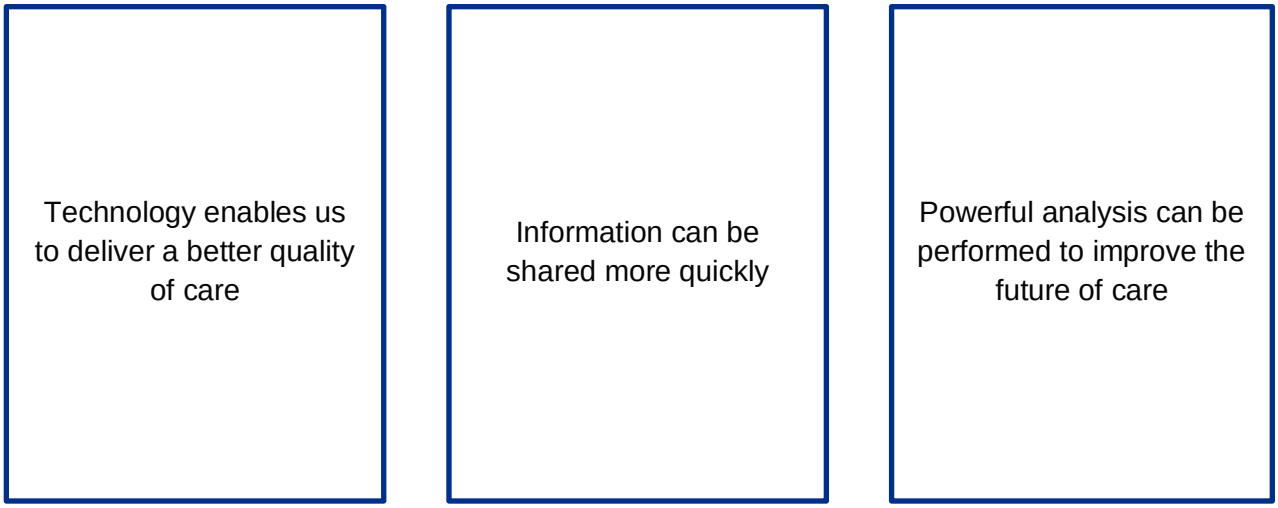
Data Security has always been important. In fact, it's no more important today than it's always been.

But it 's become more complex and time-consuming to manage now that technology is so central to the way we deliver health and care.

These technologies provide fantastic opportunities.

By an d large, technology is designed for safe and effective use. But we must ensure that we use it in a way that does not pose unacceptable risk to our business or the people in our care.

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



Safe data, safe care

Good information underpins good care.

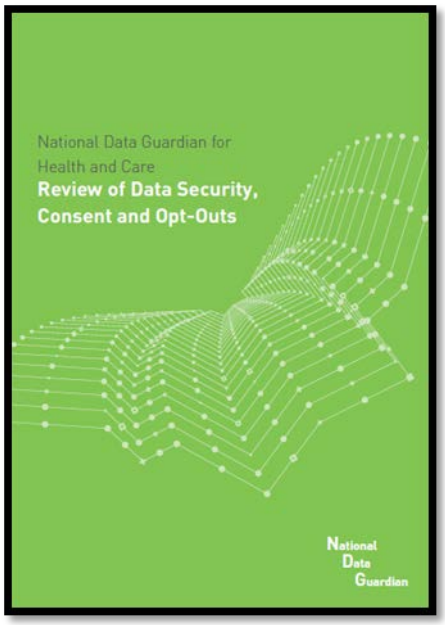
Patient and service user safety is supported when the confidentiality of personal information is maintained, its integrity is protected against loss or damage, and the information is accessible by those who are authorised.

Everyone who uses health and care services should be able to trust that their personal confidential information is protected.

People should be assured that those involved in their care, and in running and improving services, are using such information appropriately and only when absolutely necessary.

By being mindful of good practice when handling information, you can help to ensure patients and service users remain safe and receive the best possible care.

For more information please refer to:

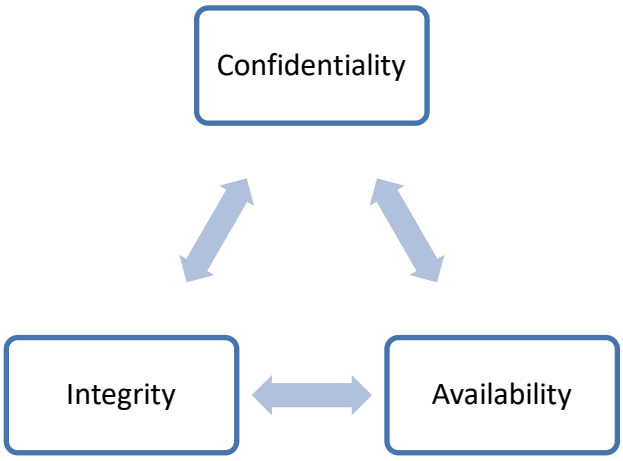


[The CQC review 'Safe Data, Safe Care’]

[The National Data Guardian Review of Data Security, Consent & Opt-Outs]

Confidentiality, Integrity, Availability

Data Security can be broken down into three areas: Confidentiality, Integrity & Availability.



Confidentiality

Confidentiality is about privacy and ensuring information is only accessible to those with a proven need to see it.

It would be unacceptable for a perfect stranger to be able to access sensitive information from a laptop simply by lifting the lid and switching it on. That's why a laptop should be password-protected and the data on it encrypted when switched off.

Integrity

Integrity is about information stored in a database being consistent and un-modified.

Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration.

Availability

Availability is about information being there when it's needed to support care.
System design must include appropriate access controls and checks so that the information in the system has consistency and accuracy, can be trusted as correct and can be relied on when providing health or care.

Scenario

Consider this scenario to illustrate the link between safe patient information and safe care. Which aspect of data security does this refer to?

Jane has an accident whilst decorating her flat and falls badly, hurting her leg. She calls the ambulance.

The paramedics ask Jane for her name, address and about her injury – they can see she is in pain and ask if she is allergic to any medications. She isn't sure if she is.

Feedback

The paramedics use their tablet device to look up Jane's Summary Care Record, which gives details of her medical history. [**Confidentiality** – the Paramedics are proven to have a need to see the record.]

However, due to a telephone network outage, they are unable to access the relevant information. The paramedics administer morphine, but Jane is allergic – a fact held on her record – and goes into anaphylactic shock. [**Integrity** – the record is correct and unmodified but was not available.]

She is driven to hospital where her condition stabilises but she is kept in intensive care

In this case, the lack of information **Availability** has had a direct impact on patient care.

Summary

This section has given you an introduction to the concepts of confidentiality, integrity and availability, and explained why data security is important to patient and service user care.

We will now look in more detail at the threats to patient and service user information and the legal obligations of all staff in health and care when accessing patient information.

When you're ready, move to the next chapter, 'Information and The Law'

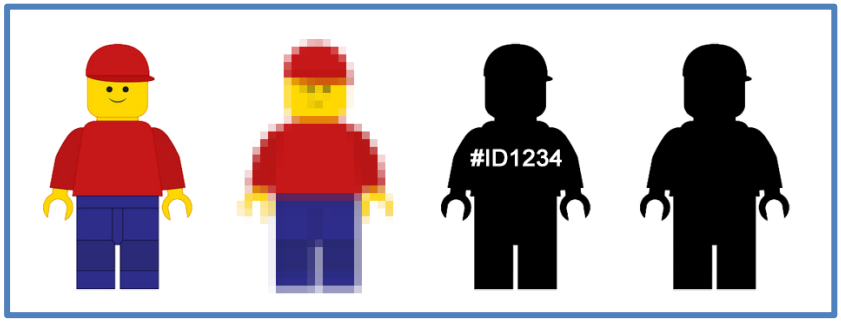
Information and the law

We will now look in more detail at managing patient and service user information in health and care. It is the law to abide by everything in this session.

We will cover:

1. Confidentiality - good practice
2. The Data Protection Act, including the rights of patients and service users
3. The Freedom of Information Act, including how to comply
4. Good record keeping

Types of information



In health and care settings, we come into contact with various types of personal information about people.

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.

Confidential information

Confidential information is information that patients and service users disclose in confidence to staff who are providing their health and care - they expect that information to be treated confidentially. It can include names and addresses, as well as a person's sensitive personal information - for example, health and care information. Other information can also be confidential information, such as employee references and some commercial information (for example, about the organisation).

Sensitive Information

As mentioned above, all health and care information is sensitive, but patients and service users may consider particular types of information to be highly sensitive, for example, information relating to their mental or sexual health.

Personal information

Information about someone is 'personal' when it identifies an individual. It may be about living or deceased people, including patients, service users, members of staff and other individuals.

A person's name and address are clearly personal information when presented together, but an unusual name may, by itself, might enable an individual to be identified.

Personal information may be recorded in hard copy or digital form – for example, photographs, videos/DVDs, whiteboards, health and care records, personnel files, on a computer – or it may be information simply known by others (such as the care team).

You may also come across the term 'personal data', which is used in the Data Protection Act 1998 and is a subset of personal information. Some personal data may be 'sensitive personal data' as it concerns a person's health and care. The Act also defines other personal data as sensitive such as religion, race and trade union membership.

Pseudonymised information

Pseudonymised information is information in which an individual's identity is disguised by using a unique identifier (that is, a pseudonym). This does not reveal their 'real world' identity, but allows the linking of different data sets for the individual concerned.

Anonymised information

This information does not identify an individual and cannot reasonably be used to determine their identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification, either by itself or when used with other available information.

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

The value of information

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

Here are some of the common ways that information is lost:

Losing information, including paper records, over the phone, via faxes, loss of computers or mobiles phones	Theft of information, such as by clicking on links to fake websites (phishing)	Insecure storage and disposal of information leading to loss or theft

Common law duty of confidentiality

Under what is known as the common law duty of confidentiality, confidential information (information that individuals disclose in confidence) should not be used or shared further without the consent of the individual.

Exceptions to the requirement for consent are limited to:

- A legal reason to disclose information, e.g. by Acts of Parliament or court orders;
- A public interest justification for breaching confidentiality such as a serious crime.

Decisions on whether or not to breach confidentiality should ideally be made by senior staff, for example your IG lead or Caldicott Guardian.

After you have completed this course, you should check what the procedure is in your organisation, so that you will know what to do if you are asked to share someone's information without their consent.

The Caldicott Principles

Before using confidential information, you should consider the Caldicott Principles:

Principle 1: **Do you have a justified purpose for using this confidential information?** The purpose for using confidential information should be justified, which means making sure there is a valid reason for using it to carry out that particular purpose

Principle 2: Are you using it because it is absolutely necessary to do so? The use of confidential information must be absolutely necessary to carry out the stated purpose.

Principle 3: Are you using the minimum information required? If it is necessary to use confidential information, it should include only the minimum that's needed to carry out the purpose.

Principle 4: Are you allowing access to this information on a strict need-to-know basis only? Before confidential information is accessed, a quick assessment should be made to determine whether it is actually needed for the stated purpose. If the intention is to share the information, it should only be shared with those who need it to carry out their role.

Principle 5: Do you understand your responsibility and duty to the subject with regards to keeping their information secure and confidential? Everyone should understand their responsibility for protecting information, which generally requires that training and awareness sessions are put in place. If the intention is to share the information, those people must also be made aware of their own responsibility for protecting information and they must be informed of the restrictions on further sharing.

Principle 6: Do you understand the law and are you complying with the law before handling the confidential information? There are a range of legal obligations to consider when using confidential information. The key ones that must be complied with by law are provided by the common law duty of confidentiality and under the Data Protection Act 1998. If you have a query around the disclosure of medical or other confidential personal information you should go to your Line Manager initially then the IG Manager if you are still not sure. For serious and complex issues your Manager should contact the Caldicott Guardian for advice and guidance.

Principle 7: Do you understand that the duty to share information can be as important as the duty to protect confidentiality? You should have the confidence to share information in the best interests of your patients and service users within the framework set out by these principles. Your organisation should support you to do so by providing you with policies, procedures and training.

Confidentiality – Good Practice

We all have a legal duty to respect the privacy of our patients and service users – and to use their personal information appropriately.

We will now look at the main aspects of confidentiality good practice by covering the following:

- Informing people
- Sharing information for care
- Sharing information for non-care

Informing People

Patients and service users will not expect health and care professionals to look at their record unless they are involved in their care. You should inform patients and service users that you are accessing and using their information.

There are specific techniques you should use when doing so.

Explain

Clearly explain to people how you will use their personal information and point them to additional information about this – for example, on your organisation's website, in a leaflet or on a poster.

Give choice

Give people a choice about how their information is used and tell them whether that choice will affect the services offered to them.

Meet expectations

Only use personal information in ways that people would reasonably expect.

You don't need to obtain consent every time you use or share personal information for the same purpose, providing you have previously informed the individual – they should know what is happening and have no objections.

Sharing information for care

Sharing information with the right people can be just as important as not disclosing to the wrong person.

Where sharing will assist the care or treatment of an individual – and it is reasonable to believe that they understand the information sharing that is needed to support that care – **you have a duty to share the information** - (this duty is set out in the Health and Social Care (Safety and Quality) Act 2015, which introduced a legal duty for health and adult social care bodies to share information where it will assist the care of an individual.)

Check	Best practices
Check that the individual understands what information will be shared and has no concerns.	Ensure that the data protection, record keeping and security best practices covered later in this workbook are met.

Respect objections

Normally, if the individual objects to any proposed information sharing, you must respect their objection even if it undermines or prevents care provision. Your Caldicott Guardian or Information Governance lead will be able to advise on what to do in these circumstances.

Sharing information for non-care

In many cases, you should obtain consent if you want to use someone's personal information for non-care purposes.

But if there is a risk of immediate harm to the patient/service user or to someone else, and you cannot find an appropriate person with whom to discuss the information request, you should share the information.

At the first opportunity afterward, you should inform the person responsible for Information Governance in your organisation so they can follow up the legal basis for sharing.

Ask	Advice	Action
Find out who is responsible for managing information sharing requests in your organisation.	Discuss the request with this person.	Provide the information only when authorised to do so.

Data protection

The Act provides people with a number of rights, the most relevant of which, in a health and care setting, are:

- The right to be informed about what their personal information is being used for and who it may be shared with (**fair processing**). When information is held in confidence, people should also be informed that they have a right to have their objection to use and sharing considered and unless there are exceptional reasons why not, to have those objections respected.
- To see and have a copy of their information (**subject to access**).
- To have objections to their information being processed considered where they claim they are suffering unwarranted distress or damage as a result.

Other rights exist and the following ones may be relevant, depending on your organisation's activities:

- To prevent processing for direct marketing.
- To object to decisions being taken by automated means.

Rights of Individuals

Patients and service users currently have many rights in relation to their information including:

- Make subject access requests.
- Have inaccuracies corrected.
- Have information erased (where it has not been relied upon to provide health or care).
- Object to direct marketing.
- Restrict the processing of their information, including automated decision-making systems or programs.

In addition to accurately recording facts, we must consider that the patient / service user might be able to view their record online.

When providing people with access, care must be taken not to reveal information that they do not already know relating to 3rd parties (e.g. information in their record about family members, other service users, etc.)

Data Protection – Good Practice

Certain simple actions can ensure that you comply with the principles of the Data Protection Act. Your organisation will have policies and procedures and can give you training to help ensure good governance of personal information.

No surprises

Handle personal information only in ways in which the individual would reasonably expect.
Think – how would you expect others to handle your personal information?

Be open, honest and clear about:

- Why you need the personal information
- What you intend to do with it
- With whom you may share it
- Who the individual should contact, if they wish to obtain a copy

Record clearly

It is important that records are full, accurate, dated and timed. They should distinguish between clinical or care findings, your opinions and any information provided by others. Be accurate:

- Enter accurate information into records and ensure the information is kept up to date
- Give individuals the opportunity to check and confirm the details held about them
- Avoid creating duplicate records

Remember – under the Data Protection Act 1998, individuals (including patients and service users) have a right to see information recorded about them. So make sure that what you record is clear and accurate.

Secure and confidential disposal

- Stick to your organisation's rules for the disposal of personal information
- Seek advice from your ICT department or provider when disposing of information held on digital assets – for example, laptops, smartphones, and so on.
- All devices such as laptops must be disposed of by your ICT department or provider.

General Data Protection Regulation

In future the General Data Protection Regulation (GDPR) will require your organisation to put stronger controls and processes in place to protect the security and confidentiality of personal data.

You can find out more about GDPR on the Information Commissioner's website at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Freedom of information

Where an organisation uses public money, the Freedom of Information (FOI) 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 requests through a number of means:

- by letter
- by email
- by fax

The Act allows anyone from anywhere in the world to ask for information held by the organisation. Individuals don't need to say who they are (other than to provide adequate correspondence details) or why they want the information. It must be provided, even if it presents the organisation in a poor light.

The Act only applies to information that already exists in a recorded form (for example, documents, emails, written notes, tape recordings). It does not normally require an organisation to create new information in order to meet a request.

Coverage – not all organisations have to comply with the Act. Is your organisation type listed below?

- Local authorities, health bodies and regulators, dentists, general practitioners, optical contractors and pharmacy businesses **must comply** with the Act.
- Private health and care providers should check their contract for any duty to comply with the Act.
- Charities and similar organisations may deal with FOI requests on a voluntary basis.

Handling Freedom of Information (FOI) requests

What you need to know:

- Handling FOI requests is a technical skill that should be handled by trained staff.
- You should not try to handle a request yourself unless you have been trained to do so.
- Many requests for information will simply be 'business as usual' requests. If in doubt, ask.

If you work in an organisation that is subject to the Act, you do have some responsibilities:

- Make sure you know who is responsible for managing requests in your organisation
- Send any FOI requests to the person responsible immediately, to comply with the 20 working day turnaround.

Example FOI request

Which one of these examples is not a valid request? Tick two options from the list below, and then go to page 20 to check your answer.		Valid	Not valid
A.	Please send me a copy of my social care record		
B.	How many GPs work in the practice?		
C.	When's my daughter's next appointment?		
D.	How much did the Trust spend on rail travel last year?		
E.	How many staff have passed their IG training?		
F.	What services are being considered for closure in the next year?		

Record keeping – Good practice

Poor quality information presents a risk to patients, service users, staff members and the organisation. If you are uncertain about any of the good practice raised in this section, talk to your line manager to improve your understanding.

Here are some checklists on what to remember.

Accurate and up to date

- Make sure you know what needs to be included in the record, why you are recording the information and how it will be used – so that the information you enter is correct and clear.
- Make sure you record the information in the correct system and in the correct record.
- Give individuals the opportunity to check information about them and point out any mistakes or inaccuracies.
- If you are not a health or care professional, you should check the information with someone who is – or cross-reference the information with other records.
- Follow your organisation's process to report and correct errors.
- Give patients or service users the opportunity to check and confirm the details held about them.
- When using shared records, ensure they are kept up to date so that other care providers have the correct information available to them.

Recorded and complete

- **Recorded as events occur** - Record information whilst the event, care or otherwise, is still fresh in your mind. Record high-risk information as a matter of urgency.

- **Complete** - Include the NHS number in health and care records (this helps to ensure that the correct record is accessed or shared for the correct patient or service user).
- **Free from duplication** - Before you create a new record, make sure that one doesn't already exist.
- **Quick and easy to locate** - Save records in a secure place that is easy to find.
- **Comply with any procedures that** ensure records are stored safely and securely, and can be quickly located when required.

Scenario

Bill has developed clinical depression since a personal tragedy, but is actively seeking treatment.

Because Bill is optimistic about a full recovery through treatment, he has not disclosed his condition to his work colleagues.

Because of a data entry error, a receptionist mistakenly calls his work number rather than his personal number and as Bill is in a meeting, one of his colleagues picks up the phone. Thinking Bill has answered, the receptionist goes on to ask him if can come in an hour earlier for his appointment.

It is immediately apparent to Bill's colleague that Bill is seeking mental health treatment, and rather than keeping the information to himself, the colleague tells other employees.

The resulting embarrassment causes Bill to resign and to make a formal complaint to the healthcare provider.

This scenario shows the importance of:

Entering information accurately into the correct systems

Verifying identity before disclosing confidential information

Example FOI Request - Feedback

Request		Valid	Not valid	Feedback
A.	Please send me a copy of my social care record		**x**	This is a Data Protection Act subject access request, the requestor should be assisted to make their request to the correct person/team
B.	How many GPs work in the practice?	**x**		This is a valid FOI request – it's not asking for information about particular GPs, just how many GPs work in the practice
C.	When's my daughter's next appointment?		**x**	Whilst this is a request for information, it is not an FOI request and it should be handled as business as usual
D.	How much did the Trust spend on rail travel last year?	**x**		This is a valid FOI request – it's not seeking information about which staff have travelled by rail but a request for the overall cost of rail travel
E.	How many staff have passed their IG training?	**x**		This is a valid FOI request – it's not a request about particular staff, it's about the number of staff that have passed their IG training
F.	What services are being considered for closure in the next year?	**x**		This is a valid FOI request – it's asking for information about decisions the organisation may have made regarding service provision

Summary

We all have a responsibility to use information lawfully. To make sure you comply with the law, you must know and comply with any Data Protection Act or Freedom of Information Act processes that your organisation has in place.

Sharing information can improve the speed and quality of service we provide to the public, so don't be afraid to share information on a need-to-know basis.

Make sure it is shared in a secure way and that, if necessary, 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.

If you are unsure, you should ask for help, or seek advice from, those who are responsible for Information Governance in your organisation.

The next section of this workbook takes a look at Data Security Threats.

Avoiding threats to data security

In this section you will look in more detail at potential threats to the security of information in the workplace.

You will learn about:

1. Social engineering.
2. Email phishing and malware.
3. Good practice for protecting information.

Social engineering

Those who want to steal data may use tricks to manipulate people to give access to valuable information. This is called social engineering.

They might try to employ confidence tricks or resort to the interception or theft of devices or documents. This includes digital or physical materials, such as printed documents or mobiles, to gain further access to more protected systems.

Criminals will often take weeks and months getting to know a place before even coming in the door or making a phone call.

Their preparation might include finding a company phone list or organisation chart and researching employees on social networking sites like LinkedIn or Facebook.

The goal is always to gain the trust of one or more of your employees, through a variety of means:

On the phone
A social engineer might call and pretend to be a fellow employee or a trusted outside authority (such as law enforcement 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? While the person asking may not seem suspicious, this is a very common tactic used by social engineers.

Online
Social networking sites have opened a whole new door for social engineering scams. One of the latest involves the criminal posing as a Facebook "friend". But you can never be certain the person you are talking to on Facebook is actually the real person. Criminals are stealing passwords, hacking accounts and posing as friends for financial gain.

The fake ICT Department

A recent scam is for criminals to set up call centres that make calls to health organisations or social care providers.

They may ask you to disclose your username, password, email address or other details about where you work. They may also try to get you to click on a malicious web or email link.

Your ICT department or provider already knows a lot about you and will not need to ask these types of questions.

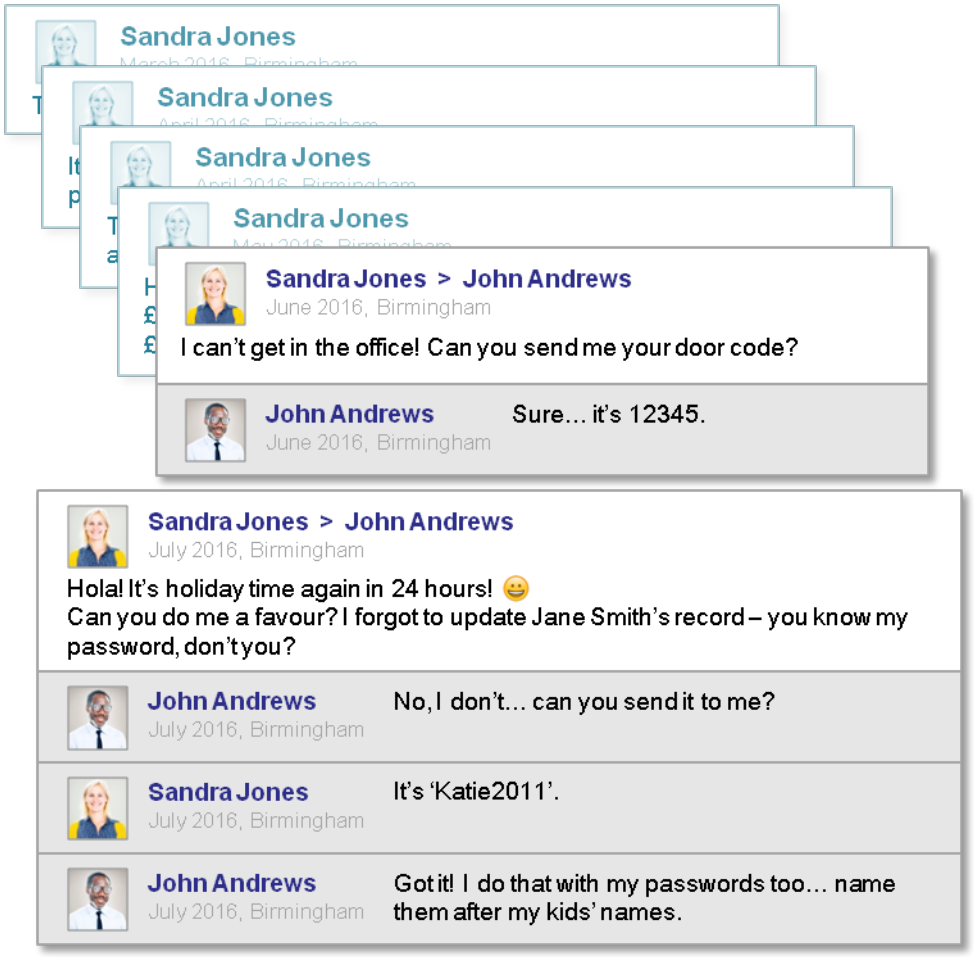
Social Engineering - what you can do

The best advice is to always be vigilant at work, whether it's using the phone, receiving unsolicited emails, using social media, or walking around your place of work.

Don't be afraid to challenge suspicious behaviour and request proof of identification, if it's safe to do so.

Using social media

Read these fictional social media posts between a mental health worker, a district nurse and their colleagues, and consider how the information could be valuable to a social engineer.



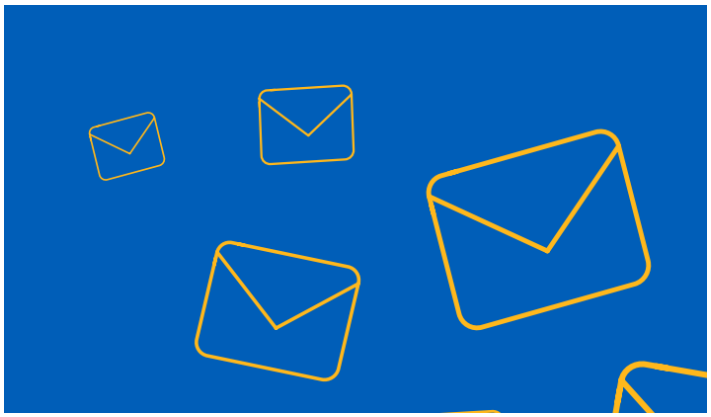
In this example, criminal could:

- Burgle Sandra's house when she was on holiday.
- Gain access to Sandra's office using the door entry code.
- Find out where the mental health worker's new office was by searching the council's website, then aligning the social worker's online pictures to their office.
- Access a computer within the building, using the mental health worker's login details to try and authorise a £50,000 transaction.
- Attempt to create a new referral for himself, to claim a personal budget.
- Access bank account details listed in the system, to steal a service user's money.

Whilst this complete scenario is unlikely to occur, a criminal could gain vital intelligence about how your organisation's processes work.

Read your organisation's social media policy to avoid any issues. If a criminal can find these posts so can your employer, which could result in disciplinary action for you.

Email phishing and malware



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 unsolicited emails containing attachments or links to try and trick people into providing access to information.

Attachments may contain a file with an **.exe** extension, these files are executable, and some may contain malicious software (malware) that will automatically download onto your computer.

This type of threat is known as **phishing**.

If you receive a request from a supposed colleague asking for login details, or sensitive, financial or patient/service user information, you should always double check the request with that colleague over the phone.

Equally if you receive an unsolicited email that contains attachments or links you have not asked for, do not open them. Remain vigilant and report the suspicious email to your ICT department or provider.

Never give your login details to anyone.

Phishing

Phishing is by far the biggest and easiest form of social engineering.

Criminals use phishing emails and websites to scam people every week. They are hoping for you to click on fake links to sites or open attachments so they can steal data or install malicious software.

The aim of phishing emails is to force users to make a mistake – for example, by imitating a legitimate company's emails or by creating a time limited or pressurised situation.

Phishing email attachments or websites might ask you to enter personal information or a password – or they could start downloading and installing malware.

Be vigilant:

- Do not install any new software unless you are advised to do so by your ICT department/provider.
- **Think** - Is someone trying to extract or extort information from you?
- If you are unsure, or think this is happening to you, then you should discuss it with your manager and ICT department/provider.

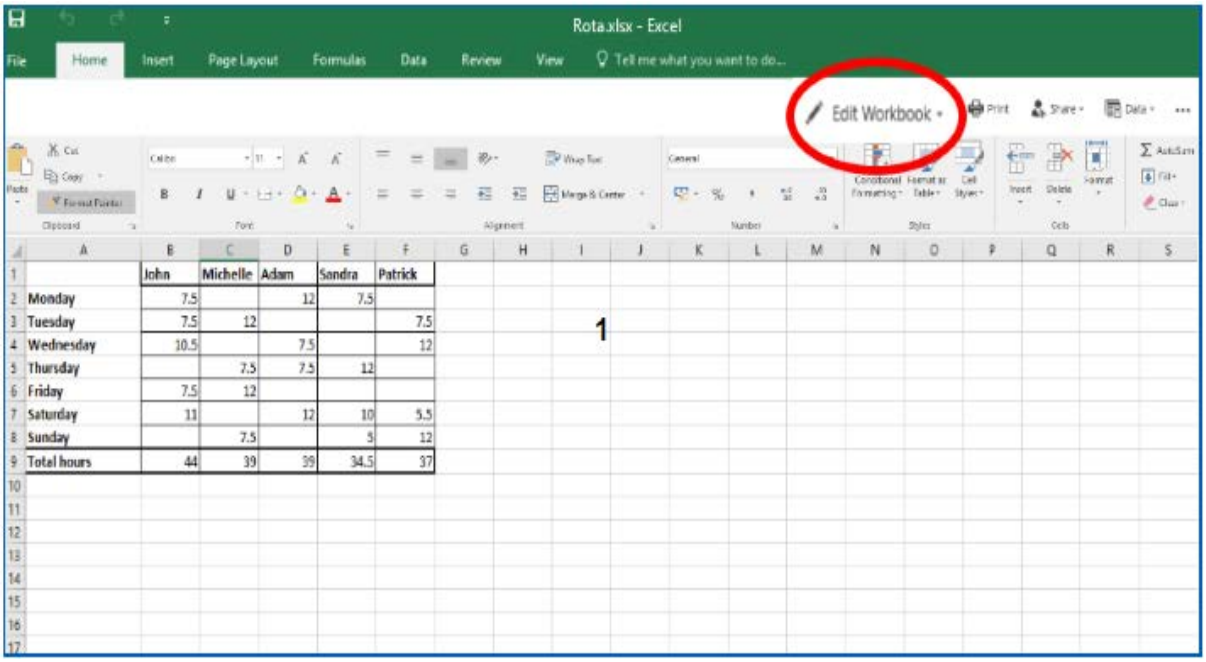
Phishing – what to do

If you do identify a phishing email, take these steps:

- Do not reply.
- Select the email, right-click it and mark it as junk.
- Ensure suspicious email domains are blocked and associated emails are sent to the spam or junk folder.
- In many cases, your organisation will have a process for dealing with spam – inform your local ICT department or provider.

Macros

Macros are a series of actions that a program such as Microsoft Excel may perform to work out some formulas. Your computer will disable macros by default because they can be programmed to install malware.



	John	Michelle	Adam	Sandra	Patrick
Monday	7.5		12	7.5	
Tuesday	7.5	12			7.5
Wednesday	10.5		7.5		12
Thursday		7.5	7.5	12	
Friday	7.5	12			
Saturday	11		12	10	5.5
Sunday		7.5		5	12
Total hours	44	39	39	34.5	37

Always be vigilant; especially when clicking 'enable macros' or 'edit document'. Do you trust the source of the document?

Malware

Malicious software (malware) can reside on your computer and evade detection, making it easier for someone to be active on your system without you noticing.

To protect your organisation from these types of threat, your ICT department or provider will ensure that you have up-to-date antivirus software installed.

Malware can make computer run slowly or perform in unusual ways. If you suspect your computer is not performing as it normally does, your ICT department or provider will be able to help.

Good practice for protecting information

Now that you've read about some of the common threats to data security in the workplace, you will look at some simple ways that you can help to ensure information remains safe.

Good practice - Setting passwords

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

Creating strong passwords doesn't need to be a daunting task if you follow simple guidelines.

The National Cyber Security Centre (NCSC) has a range of guidance on good password management, including this article to help you set secure passwords: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0.

Consider the use of a free password manager as well; again the NCSC have detailed guidance on what to look for: https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers.

Good Practice - Locking Devices

A number of simple measures can help you to stay safe online.

You should lock your device as soon as you stop using it. ALL mobile phones, laptops, PCs and tablets, whether personal or not, should have a passcode set. If you see a colleague's device open and unlocked, lock it for them and gently remind them to do so in future.

This also applies to corporate mobile devices - activate the lock function so that a password or code is needed to unlock them.

Tip: select the Windows Key + L on your keyboard to quickly lock your laptop or PC.

Good practice - Removable drives

Do not use unauthorised USB drives and avoid plugging in any non-approved devices to charge via a USB cable. A private mobile phone is effectively a large USB storage device and may contain malware.

Before using USB drives, scan them to ensure they are safe. A USB device can technically be a small computer. If you plug the USB into an untrusted computer, malicious software could be transferred and passed on to any other devices where you use the USB.

Ask your ICT department or provider if you are unsure.

Good practice - Untrusted websites

Be vigilant when you visit a website that is declared "untrusted".

If a web browser states that you are about to enter an untrusted site, be very careful – it could be a fake phishing website that has been made to look genuine.

A browser may display a red padlock or a warning message stating ‘Your connection is not private’."

Good practice - Mobile devices

Digital Do’s

- Do read, understand and comply with your organisation's policy and procedures regarding the use of digital assets.
- Do seek advice from your line manager if any aspects of the policy or procedures are unclear.
- Do store your digital assets securely when not in use.
- Do update antivirus software if your digital asset prompts you to do so.
- Do keep regular backups of the data stored on digital assets – store appropriately, according to your organisation’s policies.
- Do report any lost or stolen digital asset to the police immediately – you should also follow your organisation’s incident management procedure.
- Do ensure that digital assets and passes are handed back if you are leaving the organisation.

Digital don’ts

- Don’t use your own device for business purposes unless this has been properly authorised.
- Don’t use work-provided digital assets for personal use (such as social media and personal web browsing) unless you are authorised to do so.
- Don’t connect your work-provided digital asset to unknown or untrusted networks – for example, public Wi-Fi hotspots.
- Don’t allow unauthorised personnel, friends or relatives to use your work-provided digital assets.
- Don’t attach unauthorised equipment of any kind to your work-provided digital asset, computer or network.
- Don’t remove or copy personal information, including digital information (such as by email, on a USB stick), off site without authorisation.
- Don’t leave digital assets where a thief can easily steal them – for example, on display or unattended in your car or in a public place.
- Don’t install unauthorised software or download software or data from the internet.
- Don’t disable the antivirus protection software.

Good practice - Disposal of confidential information

We have to be careful when disposing of any information. Much of the data that health and care organisations create and use is classed as **Official** in the eyes of the government.

OFFICIAL - Government Definition
The majority of information that is created or processed by the public sector: This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media.

Special care must be taken to securely dispose of the following things, including but not limited to:

- Paper records that contain confidential information
- Desktop computers
- Servers
- Multifunction devices (e.g. Printers/Photocopiers)
- Laptops, tablet computers and electronic notebooks
- Mobile telephones
- Digital recorders
- Cameras
- USB devices
- DVDs, CDs and other portable devices and removable media.

Your organisation will have a process for securely disposing of each of these things to avoid breaches.

Good practice - Clear desks

Most organisations now have policies about having clear desks which you should be aware of. This is because things tend to get lost on cluttered desks.

Do not leave information in unsecure locations. For example, documents that identify someone, financial information and so on.

Having a clear desk ensures that you are not potentially leaving sensitive information laying around, raising the risk of a breach.

Summary

In this section you have learnt about different types of data security threat, how to spot them, and what to do. The learning also covered good practice in the workplace.

The last section covers what to do if you identify that a security incident or breach has occurred.

Breaches and incidents

This section will look at some scenarios for breaches and incidents and explain how to avoid them.

In your place of work, you must be able to spot common activities where information could be lost, and know what to report. All members of staff provide our first line of defence against information loss and theft.

The section covers:

- Identifying breaches and incidents
- Reporting breaches and incidents
- Avoiding breaches and incidents
- Everyday scenarios where information can be lost.

You've already looked at a number of ways in which data security might be compromised.

Such incidents typically fall into two categories:

- A **breach** of one of the principles of the Data Protection Act 1998 and/or confidentiality law
- Technology-related **incidents**

A breach can be caused by a security incident (for example, disclosure of patient details using social media). However, some incidents (for example, defacing a website) may not involve a breach of information.

More information about the different types of incidents is in the table below.

Breaches	**Cyber incidents**
Identifiable data lost in transit	Phishing email
Lost or stolen hardware	Denial of service attack
Lost or stolen paperwork	Social media disclosure
Data disclosed in error	Website defacement
Data uploaded to website in error	Malicious damage to systems
Non-secure disposal – hardware	Cyber bullying
Non-secure disposal – paperwork	
Technical security failing	
Corruption or inability to recover data	
Unauthorised access or disclosure	

Breaches

The Information Commissioner reports on trends in breaches and incidents: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

In health and care the most common forms are:

- Faxes that are sent to the wrong number or misplaced.
- Lost or stolen paperwork.
- Failure to adhere to principle 7 of the Data Protection Act 1998.

Incidents using technology

Website defacement
This term is used to describe an attack on a website that changes the content of the site or a webpage. It may also involve creating a website with the intention of misleading users into thinking that it has been created by a different person or organisation.

Social media disclosure
This term is used to describe the disclosure of confidential or sensitive information by an organisation's employees through a social media site.

Denial of service attack
This term is used to describe an attempt to make a machine or network resource unavailable to its intended users.

Malicious damage to systems
This term is used to describe what happens when a person intentionally sets out to corrupt or delete electronic files, information or software programs.

Consequences of breaches and incidents

Imagine the risk of making an important decision about a person's care if their record was no longer available, was wrong or incomplete - or if someone had tampered with it.

By this point in the course you should understand why data security measures are in place. We all need to help ensure that our information is protected in the best way possible.

Reporting incidents

You have a responsibility to...

Know how to report data security incidents:

- If you know or suspect that an incident has taken place, register it in line with your organisation's incident reporting procedure.
- If an individual deals with such data security incidents in your organisation, notify them as soon as possible, so they can assess how serious the incident is and start an investigation.
- Know your organisation's policy on the fair use of ICT– do not alter or change any software on your device without permission.

Report suspected incidents and any 'near misses':
Lessons can often be learned from them – they can be closed or withdrawn when the full facts are known.

Data security risks - Scenarios

Certain procedures can help to reduce the risk of sending information by post, email, telephone and fax.

Consider these scenarios and the different ways in which breaches and incidents can be avoided by remaining vigilant and aware of your personal responsibility.

Postal breach

Consider the following scenario which illustrates how incidents can arise using the post.

The situation - Miss Broom is waiting to receive information from her social worker. She opens her post one morning and finds that, as well as her own letter, the envelope contains two further letters addressed to other people.

Miss Broom contacts the organisation and tells an administrative officer about the additional letters. She receives an apology and the promise of a call back.

The organisation's reaction - The organisation's information governance lead telephones Miss Broom to apologise for the error and asks her to keep the letters safe whilst arrangements are made for someone to collect them.

Consequences - The organisation wrote a formal apology to Miss Broom and to the two individuals that she received letters about. Both individuals were deeply concerned that Miss Broom (who they did not know) now knew important information about them. One of them wrote to their local paper about the breach.
Senior staff in the local authority spent the next two weeks responding to media queries about the number of breaches the organisation had experienced. The other individual, who had suffered from a similar breach the previous year, instructed his solicitor to bring legal proceedings against the local authority.

If you are placed in this situation, follow your organisation's procedures and, where possible, adhere to the following principles.

- Address personal information to a named person
- Consider using tracked or recorded delivery for personal information
- Case notes should only be sent in robust approved packaging

Email breach

The situation - Mr. Foster has recently been diagnosed with depression and has joined a support group to help him through his care.
The organisation emails information to support group members each month. Recently, they have started to receive emails and phone calls from individuals who are upset about the disclosure of their names and email addresses to more than 500 people.

The organisation's reaction - The organisation undertakes an investigation and finds that a new member of staff had sent out the email. They had mistakenly put the list of all the support group members' email addresses in the 'CC' field – rather than the 'BCC' field – of all the individual emails.

Consequences - Everyone who received the email could identify who was a member of the depression support group. The investigation also finds that all existing staff members involved in sending out emails knew what to do, but had not supervised the new member of staff.

Your organisation will have guidance on sending secure emails. If you are an NHSmail user you can go to the NHSmail portal (http://support.nhs.net/policyandguidance) to access guidance about sending emails securely.

If you are placed in this situation, follow your organisation's procedures and:

- Make sure you know the difference between 'TO', 'CC' and 'BCC'.
- Check email content and distribution before you click 'Send'.
- Be aware that some people may share their email accounts so the content may need to be adjusted.

Email checklist

Before emailing any external parties:

- Check with your line manager and/or information governance lead whether it is acceptable to send personal information in this way.
- Confirm the accuracy of the email addresses for all intended recipients, sending test emails where unsure.
- Check that everyone on the copy list has a genuine 'need to know' the information you intend to send.
- When referring to patients or service users use the minimum identifiable information (e.g. NHS number).

- Check whether you need to encrypt the email yourself or the recipients are all using secure interoperable email systems, e.g. NHSmail-to-NHSmail or to Government Secure Internet (GSI) systems (ask your IT support if you don't know).
- Where email needs to be sent to an unsecure recipient check whether this is at the request of a service user who understands and accepts the risks or if encrypting the email yourself is more appropriate.

Phone breach

Consider the following scenario which illustrates how incidents can arise using the post.

The situation - Joe, a practice manager, receives a call from a local hospital requesting information about Mrs Smith, one of the practice patients. He knows she has been referred to that hospital for cancer investigation so he gives the information to the caller.

The result - The next morning, Mrs Smith phones the practice and tells Joe that her brother-in-law has information about her health that he can only have obtained from the practice. At that point, Joe realises he had no proof that the previous day's call was from the local hospital.

Phone checklist

If a request for information is made by phone, where possible:

- Confirm the name, job title, department and organisation of the person requesting the information.
- Confirm the reason for the information request is appropriate.
- Take a contact telephone number, e.g. main switchboard number (never a direct line or mobile phone number).
- Check whether the information can be provided – if in doubt, tell the enquirer you will call them back.
- Provide the information only to the person who requested it (do not leave messages).

Ensure that you record your name, date and the time of the disclosure, the reason for it and who authorised it – also record the recipient's name, job title, organisation and telephone number.

Fax breach

You should never send personal information by fax unless it is absolutely necessary. Some organisations use multi-function printers (photocopiers) to send faxes; this rule also applies to these devices. Consider the following scenario which illustrates how incidents can arise using fax.

The situation - Rachel works in a care home and is asked to fax some service user information to a local general practice. However, she is in a rush and accidentally gets one of the numbers wrong.

What happens - The fax goes to a local golf club where the manager calls the local newspaper. An embarrassing article about negligence and breach of confidentiality soon follows.

The consequences - This is not the first such error made by Rachel's organisation and the Information Commissioner's Office, once informed, carries out an investigation that results in a £100,000 fine.

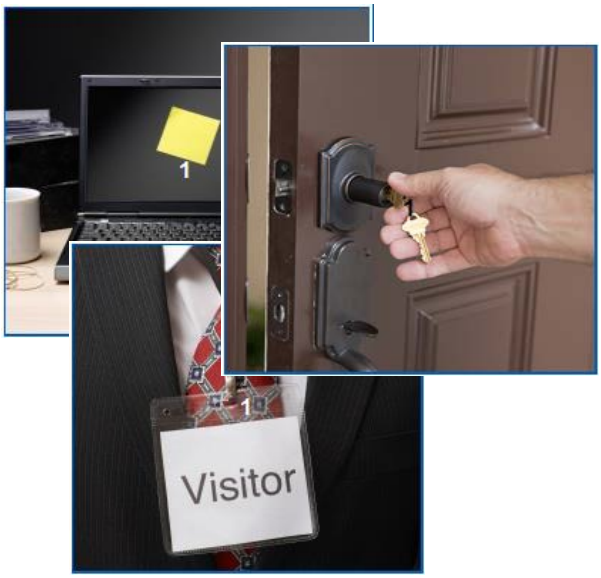
Fax checklist

If it is absolutely necessary to send information by fax, use the following procedure where possible:

- Personal details should be faxed separately from clinical details with the exception of the NHS number.
- Telephone the recipient of the fax (or their representative) to let them know you are going to send confidential information.
- Ask the recipient to acknowledge the fax.
- Double check the fax number and use pre-programmed numbers.
- Make sure your fax cover sheet states who the information is for, and mark it 'Private and Confidential'.
- Either request a confirmation that the transmission was completed or call to confirm.
- Make sure you remove the original document from the fax machine once you have sent the fax.

Fax machines used for sensitive information should be sited in a 'safe haven' location - in a room with access controls, not in reception or in front of clear-glass windows or public-accessible areas.

Data security risks



Last week, someone in a high visibility vest visited a Social Care office as well as a GP practice. He followed a member of staff into the building and told the receptionist that he needed everyone's details for a 'software update'. He then sold these details to other criminals. Let's find out what else he found.

Doors

Nearly every door he encountered in the office was open. Even those doors marked as "restricted access" had been propped open to allow for a delivery.

Visitors

When he was at the reception desk, he asked for directions to the server room. The receptionist was happy to help…he wasn't even asked to sign in or show a visitor's badge.

Desks

Despite most organisations having strict clear desk policies it was amazing how much information he could find in unoccupied office areas. He had a bag of memory sticks and randomly dispersed them around the desks in the hope that someone will plug one into their machine. Once plugged in, it will start installing malware into the computer.

Other areas

He then gains access to the server room as the door has been left unlocked…from here, the possibilities are endless.

With this access, he can disrupt the server as much as he likes, causing connectivity problems across the whole organisation.

As there is so little **physical security**, he can potentially come and go as he pleases…perhaps next week.

Summary

In this workbook, you've looked at why data security is important, the legal obligations for staff working in health and care, threats to the security of information, and how to identify a potential incident or breach.

Hopefully you can now see why good data security is important, and why we are all bound by legal requirements to protect health and care information.

You should now complete the assessment to finish your training.

Module summary

Having completed this session, you should understand:

- The principles and terminology of information governance (IG).
- Basic data security / cyber security terminology.
- The importance of data security to patient/service user care.
- That law and national guidance requires personal information to be protected.

And be able to:

- Explain your responsibilities when using personal information.
- Identify some of the most common data security risks and their impact.
- Identify near misses and incidents and know what to report.
- Distinguish between good and poor practice when using personal information.
- Apply good practice in the workplace.

Resources

You can refer to the following for additional information:

1. The NHS Care Record Guarantee[1]. London: NIGB, 2011.
2. Department of Health. Information Security Management: NHS Code of Practice[2]. London: DH, 2007.
3. Records Management Code of Practice for Health and Social Care 2016[3] IGA, 2016
4. Website of the Information Governance Alliance[4]
5. Caldicott 1 - Report on the Review of Patient-Identifiable Information[5]. London: Caldicott Committee, 1997
6. Caldicott 2 - Information: To Share Or Not To Share? The Information Governance Review[6]. London: Independent Information Governance Oversight Panel, 2013
7. Caldicott 3 - Review of Data Security, Consent and Opt-Outs[7]. London: National Data Guardian, 2016

References

8. Information Commissioner's Office. Trends in breaches and incidents[8]
9. Department of Health. Confidentiality: NHS Code of Practice[9]. London: DH, 2003.
10. The National Cyber Security Centre - Creating passwords[10]
11. The National Cyber Security Centre - Password Managers[11]

[1] http://systems.digital.nhs.uk/rasmartcards/documents/crg.pdf
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200506/Information_Security_Management_-_NHS_Code_of_Practice.pdf
[3] http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf
[4] https://digital.nhs.uk/information-governance-alliance
[5] http://ukcgc.uk/docs/caldicott1.pdf
[6] https://www.gov.uk/government/publications/the-information-governance-review
[7] https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs
[8] https://ico.org.uk/action-weve-taken/data-security-incident-trends/
[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
[10] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[11] https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

Assessment

Attempt **all** of the following **15** questions, and check with your IG lead whether your responses need to be recorded and logged

Question 1: Which of the following statements on the types of information used in health and care is **correct**? Tick **one option** from the answers listed below.		
A	Personal information applies only to living people	
B	Personal information applies only to patients	
C	A person's name and address are needed for them to be identified	
D	An unusual name will not identify an individual	
E	Anonymised information cannot be personal or confidential	

Question 2: Which of the following statements on the topic of confidentiality is **correct**? Tick **one option** from the answers listed below.		
A	It is not necessary to explain how someone's personal information will be used	
B	It is not necessary to give them a choice about how their personal information is used	
C	It is not necessary to tell them before their personal information is shared for the first time	
D	It is not necessary to get consent every time you subsequently share someone's personal information for the same purpose	

Question 3: Which of the following statements on the Data Protection Act 1998 is **correct**? Tick **one option** from the answers listed below.		
A	The Act only applies to patient or service user information	
B	The Act only applies to personal information in digital form	
C	The Act prevents information being shared for health and care purposes	
D	Organisations can be fined or face legal action for breaching the principles of the Act	

Question 4: Which of the following statements on the Freedom of Information Act is **correct**? Tick **one option** from the answers listed below.		
A	The Act puts a duty on organisations to supply information to individuals who make a written request	
B	Individuals can submit a request for information in writing or over the telephone	
C	Organisations must respond to a valid request within 10 working days	
D	If necessary, organisations have a duty to create new information in order to meet a FOI request	

Question 5: Which of the following represents an example of good practice in record keeping? Tick **one option** from the answers listed below.		
A	Storing commonly used records in your drawer	
B	Including each person's NHS number	
C	Creating duplicate records for each person	
D	Preventing people from checking their own details	
E	Updating records at the end of each month	

Question 6: Which of the following represents an example of good practice in physical security? Tick **one option** from the answers listed below.		
A	Having a sign-in procedure for visitors	
B	Sharing your ID badge with a colleague who has forgotten his	
C	Propping open fire doors when the weather is warm	
D	Leaving service user records on your desk in case you need them later	

Question 7: Which of the following should not be used to send personal information unless absolutely necessary? Tick **one option** from the answers listed below.		
A	Post	
B	Email	
C	Fax	
D	Telephone	

Question 8: Which of the following is likely to **increase** the risk of a breach when sending personal information? Tick **one option** from the answers listed below.		
A	Using a trusted postal courier service	
B	Verifying the identity of telephone callers	
C	Using a secure email system	
D	Leaving messages for telephone callers	
E	Encrypting any personal information	

Question 9: Which of the following statements best describes how to respond to an incident? Tick **one option** from the answers listed below.		
A	All incidents should be reported	
B	An incident should be reported only if it results in personal information being revealed	
C	An incident should be reported only if it results in personal information being lost	
D	An incident should be reported only if it results in harm to a service user	
E	There is no need to report an incident	

Question 10: Which of the following is **least** likely to create a security risk? Tick **one option** from the answers listed below.		
A	Leaving sensitive documents on your desk	
B	Using a company USB at work	
C	Using an unauthorised mobile phone for work matters	
D	Leaving a restricted access door open	

Question 11: Which of the following is characteristic of a secure password? Tick **one option** from the answers listed below.		
A	No more than 5 characters in length	
B	Contains your username	
C	Contains a mix of character types	
D	Similar to previous passwords	

Question 12: Under which of the following circumstances is it acceptable to use your work-provided digital asset for personal browsing? Tick **one option** from the answers listed below.		
A	To connect to your personal webmail	
B	If you don't stay online too long	
C	When you are working outside the office or home	
D	Only if you have been authorised to do so by your organisation	

Question 13: Which of the following is the best course of action if you receive a phishing email? Tick **one option** from the answers listed below.		
A	Reply to the email	
B	Forward the email to your colleagues	
C	Notify your IT department/provider	
D	Open the attachments	
E	Click on the links in the email	

Question 14: Consider the following statement. “If your computer is running slowly you should disable the anti-virus software.” Tick **one option** from the answers listed below.		
A	This statement is true	
B	This statement is false	

Question 15: Which of the following represents an example of good practice in data security? Tick **one option** from the answers listed below.		
A	Attaching unauthorised equipment to your work-provided digital asset	
B	Updating the anti-virus software on your work-provided digital asset	
C	Using your work-provided digital asset for personal reasons not consistent with your organisation’s policy	
D	Downloading software or data from the Internet to your work-provided digital asset	
E	Connecting your work-provided digital asset to an unknown network	

You have reached the end of this workbook.