IG and Data Security Essentials Workbook

Name:

Job role:

Department:

Contents

IG and Data Security Essentials Workbook

Instructions

This workbook is divided into two parts. Please read the description to find out if you should complete **one or both parts**.

Part 1 Focuses on information governance essentials i.e. general aspects of using information and includes some common data security topics.

Part 2 Focuses on aspects of using digital information i.e. data and cyber security.

Intended audience

All staff should complete **Part 1.**

Staff who use IT equipment (also known as digital equipment or assets) at work should complete **Parts 1 and 2.**

Part 1 - Description

In this session you will learn why information governance is important and understand your responsibilities when using personal and anonymised information.

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

Duration: Approx. 30 minutes

Learning Objectives

By the end of this session you will understand:

- The principles and terminology of information governance (IG).
- That health and care personal information is valuable.
- That law and national guidance requires personal information to be protected.
- Your responsibilities when using personal information.

And be able to:

- 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.
- Apply good practice in the workplace.

Introduction

In this session, we will explore the practical steps you should take to protect personal information and to make sure it is only used and shared in the right way. In other words, we will learn how to practise good information governance.

This means we'll look at:

- How to share information appropriately whilst respecting people's confidentiality.
- What you need to do to comply with the law on data protection and freedom of information.
- Good record keeping processes, including information quality.
- Information security.
- Some common data security risks and how to avoid them.

NHS Case Study

Hundreds of data incidents involving public sector and commercial organisations happen every year.

Fig 1 Hundreds of data incidents happen in the UK every year

In 2016, an NHS Trust was fined £180 000 by the Information Commissioner after revealing the email addresses (many of which included names) of over 700 users of a HIV service. See: https://ico.org.uk/action-weve-taken/enforcement/chelsea-and-westminster-hospital-nhs-foundation-trust/.

In response to this and similar incidents, the National Data Guardian[1] (Dame Fiona Caldicott) highlighted that:

- People expect that what they tell their health or care professional will remain confidential.
- There should be no surprises for patients or service users about how their information is used.
- Much more needs to be done to earn the trust of patients and service users.
- Whilst there are examples of good practice there are still issues caused by people, processes and technology.

In this session, we will look at how to make sure you follow the right processes and procedures when you use personal information.

Key roles

Depending on the size of your organisation there is likely to be one or more people in key roles to help you follow the right processes and procedures when you use personal information. It is important that you find out which people are in these key roles in your organisation, so that you know where to obtain advice on IG and related issues.

These roles may differ depending on the type of organisation you work in.

Caldicott Guardian – this is usually a senior health or care professional in large to medium sized organisations. They are responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

Senior Information Risk Owner – the SIRO is responsible for overall management of information risks in large to medium sized organisations.

Privacy officer – many organisations will be using the Summary Care Record[2] - an electronic record of important patient information, created from GP medical records. These organisations will have at least one person with the privacy officer role who is responsible for monitoring access and can generate audits and reports.

[1] https://www.gov.uk/government/organisations/national-data-guardian
[2] https://digital.nhs.uk/scr

Information Governance lead – an IG lead in a large to medium sized organisation will be responsible for coordinating information governance. In a smaller organisation, they are likely to be responsible for all of the key roles.

Types of information

In health and care settings, we come into contact with lots of types of information about people. These can be categorised as:

- Personal information
- Confidential information
- Anonymised Information, and
- Pseudonymised information

Fig 2 It is important to be able to differentiate between different types of information

Personal information

Information about someone is personal information when it **identifies an individual**.

It may be about living or deceased people, including patients, service users and members of staff.

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

Personal information may be recorded in hard copy or digital form, e.g. photographs, videos/DVDs, whiteboards, health and care records, personnel files, on a computer, or simply known by others (e.g. 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 is about a person’s health and care.

Confidential information

Confidential information is information that patients and service users disclose in confidence to staff providing their health and care and expect that information to be treated confidentially.

It can include names and addresses as well as a person’s sensitive personal information, e.g. health and care information.

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.

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

Pseudonymised information

Pseudonymised information is data in which individuals are distinguished by using a unique identifier (i.e. a pseudonym). This does not reveal their ‘real world’ identity.

Information that has been adequately pseudonymised is anonymised data in the hands of a recipient; however, they usually can be re-identified by the original holder of the data using the pseudonym.

Why do I need to know this?

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. If you work in the health or care sector you will come across these types of information when:

- Providing treatment, care, support, advice or other services directly to patients or service users.
- Overhearing personal information whilst you carry out your job.

- Taking the right patient or service user to the right place at the right time.
- Arranging appointments, running clinics and sending out communications.
- Recording and sharing information in systems.
- Providing IT and other support services to health and care staff.

No matter what your job is, you have a legal duty to maintain the confidentiality of information you see or hear and keep it secure.

Question - Characteristics of Information

Consider the characteristics of information. Tick the most appropriate type of information for each statement. Then go to page 45 to check your answers.

Characteristics		Personal	Confidential	Anonymised	Pseudonymised
A.	Is about a named individual's next hospital appointment				
B.	The information does not directly identify an individual				
C.	Might include names and addresses				
D.	No-one can link the information back to a specific individual				
E.	Identifying information will have been replaced with a code				
F.	The information directly identifies particular individuals				

The value of information

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

Organisational value

Information is vital to an organisation, without it an organisation would be unable to carry out its functions. When the information is about patients or service users, any issue that disrupts its availability or compromises its accuracy can impact on the ability to provide a health and care service.

Therefore we must all follow the right processes to protect patients and service users and their information.

Fig 3 Information is vital to an organisation, without it an organisation would be unable to carry out its functions

Why steal information?

There are many reasons why data information might be stolen including:

- To blackmail or bribe someone.
- For profit or gain.
- To compile a database.
- To cause reputational damage to the organisation.

Theft can be undertaken by someone within or external to your organisation.

What is the impact on individuals?

Think about the details held by a high street bank. If these are stolen and misused, the fraud is relatively quickly noticed and steps taken to prevent further fraud.

Health and care records contain not only personal details such as names and addresses but also sensitive care information. This could include confidential details of illnesses and diagnoses, or advice about sensitive matters, or care and treatment of a highly private nature. This information could be used to:

- Set up false identities.
- Misuse existing identities to obtain multiple drug prescriptions and treatment which may then be recorded on the real person's record.
- Sell the information to unscrupulous 3rd parties to identify people vulnerable to blackmail, extortion or targeted marketing.

The theft and compromise of an individual's lifetime record of health and care cannot be resolved by simply closing an account. The impact on the individual can be devastating. It will cause long-lasting reputational damage to an organisation that failed to protect these confidential records.

Imagine if your records were stolen and how this could affect you…

Confidentiality

Patients and service users trust us to respect their confidential information at all times. Staff have a duty to treat personal information with confidentiality. In the NHS this duty is set out in the Confidentiality NHS Code of Practice[3]. For social care staff the duty is in the Skills for Care Code of Conduct[4].

Registered and regulated staff members, such as social workers, pharmacists, doctors and nurses, also have a duty to follow their professional codes of practice which will include a duty of confidentiality.

Fig 4 NHS and care organisations have a duty to treat personal information with confidentiality

Consider the following scenario on the importance of respecting people's confidentiality.

You are at work when you see your neighbour arrive for an appointment. You see no harm in looking at her record as you have a duty of confidentiality. Later, you bump into your neighbour, and while chatting she begins to suspect that you know what her appointment was about. She suspects her confidentiality has been breached and tells your organisation of her suspicions. A day later, your line manager asks you to explain your access to her record.

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
[4] http://www.skillsforcare.org.uk/Standards-legislation/Code-of-Conduct/Code-of-Conduct.aspx

Your line manager tells you that the breach of confidentiality must be reported. Your neighbour will be informed and may complain more formally and even take legal action. He also says you have breached the organisation's policies and may be subject to disciplinary proceedings. If you are a registered or regulated professional you could also be reported to your regulatory body, which may result in suspension or removal from the professional register.

Your neighbour's loss of trust in you and the organisation could result in her no longer attending for her appointments or being unwilling to reveal important care information. In turn, this could affect the care, advice or treatment she receives.

Confidentiality - Good practice

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

Fig 5 Good practice in confidentiality includes gaining permission from the patient or service user and sharing information appropriately

Informing people

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

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

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

In the previous scenario, your neighbour would not expect you to look at her record unless you were involved in her case.

You don't need consent every time you use or share personal information for the same purpose, as long as you have previously informed the individual so they know what is happening and have not objected.

Sharing information for care purposes

Sharing information with the right people can be just as important as not sharing it with the wrong people. Where sharing will assist the **care or treatment** for an individual and it is reasonable to believe that they understand the information sharing that is needed to support that care or treatment, you have a duty to share the information.

Best practice is still to:

- **Check** that the individual does **understand** what information will be shared and has no concerns.
- Ensure the data protection, records keeping and security **best practices** covered later in this session are met.

If the individual objects to any proposed information sharing you must normally 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 purposes

Get people's **consent** if you want to use their personal information for **non-care purposes**.

In the previous scenario, you were not part of the care team involved in your neighbour's care, so you would need her explicit consent to look at her record.

There are exceptions to this general rule, but **you should not make decisions on whether or not consent is required** unless you are qualified to do so.

If you are asked for personal information but are not sure whether you can share it, you should:

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

If you cannot find an appropriate person to discuss an information request with, you should carefully consider if there is an immediate risk of harm. If so, you may need to share first and be able to justify your actions later. Inform your Information Governance lead at the first opportunity to follow up the legal basis for sharing.

Question - Informing people

Which of the following can help to keep people informed about how their personal information? Tick one or more of the options from the list below, then go to page 45 to check your answers.

Options		
A.	Sit down and explain it to them directly	
B.	Direct them to the relevant section on your organisation's website	
C.	Give them a leaflet explaining such matters	
D.	Tell them about their information sharing choices	
E.	Get their consent to use their information where necessary	

Question - Information request

You receive a request for some personal information but are not sure whether you can share it. Which of the following is the best course of action? Tick one of the options from the list below, and then go to page 45 to check your answer.

Options		
A.	Provide the information as requested, it's probably alright	
B.	Find out who is responsible for managing information sharing requests in your organisation	
C.	Tell the requestor that they cannot have the information under any circumstances	

Data Protection Act 1998

The Data Protection Act 1998 contains a set of principles for managing **personal data** about **living** individuals.

The Act does not prevent information being shared for health and care purposes but it contains a set of rules that must be followed for the use and sharing of personal information to be fair and lawful.

Fig 6 Organisations must comply with a set of rules on the use and sharing of personal information

Legal rights

The Act provides people with a number of rights; the most relevant 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 their objections respected.
- The right to see and have a copy of their information (**subject access**).
- The right to have their 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:

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

Enforcement

An individual and/or the organisation they work for can be fined for breaching one of the Principles of the Act or legal action can be taken against them.

The Information Commissioner's Office has a number of powers it can use against organisations and individuals including: These include:

- Prosecuting an individual (employee) who has committed a criminal offence under the Act, such as obtaining or disclosing personal data without the consent of the data controller (their employer). This can result in the individual receiving an unlimited fine.
- Issuing a Monetary Penalty Notice to an organisation who has committed a serious breach of the Act. This can result in the organisation being fined up to £500,000.

Data Protection - Good practice

Certain simple actions can ensure that you comply with the principles of the Data Protection Act.

Fig 7 Good practice in data protection includes the need for information to be recorded accurately and the disposal of confidential information

No surprises

- Handle personal information only in ways the individual would reasonably expect.
- **Think:** How would you expect others to handle your personal information?

Be open, honest and clear

- Be clear about:
    - Why you need the personal information.

- What you intend to do with it.
- Who you may share it with.
- Who the individual should contact if they wish to obtain a copy.

Make sure you need it

- Do not collect or hold personal information ‘just in case it might be useful one day’.

Record clearly

- It is important that records are full, accurate, dated and timed, and distinguish between clinical or care findings, your opinions and information provided by others.
- This is particularly applicable to making decisions about a child’s or young person’s safety or welfare.

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 that under the Data Protection Act 1998, individuals (including patients and service users) have a right to see information recorded about them. So make sure 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 IT department or provider when disposing of information held on digital assets, e.g. laptops, smartphones, etc.

Your organisation will have **policies**, **procedures** and will provide you with **training** to help ensure good governance of personal information.

Question - Data Protection Act

Consider the following statement - ‘The Data Protection Act prevents information from being shared for health and care purposes’. Tick one of the options below, and then go to page 45 to check your answer.

Options		
A.	This statement is true	
B.	This statement is false	

The Freedom of Information 2000

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.

Fig 8 Public sector organisations have a duty to provide information in response to a written request

-

Examples of FOI requests

Valid example: A written request asking what homecare services are available in the area and if there are any plans to change the service levels.

Valid example: A written request asking how many data breach incidents have been reported each year for the past 3 years.

Valid example: A patient's letter of complaint following a breach of their information which also asks for a copy of the organisation's confidentiality policy.

Invalid example: A telephone call asking what homecare services are available in the area and if there are any plans to change the service levels.

Handling FOI requests

FOI is a technical subject that should be handled by trained staff. You should not try to handle a request yourself unless you have been trained to do so or have been authorised by a senior manager due to pressure to meet the 20 working day deadline.

Your responsibilities

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

- **Provide advice and assistance:** Requests must be in writing and should contain sufficient information to enable the requested information to be found - where necessary you should assist the individual to put their request in writing
- **Make sure you know who is responsible for managing requests in your organisation:** The timescales for complying are within 20 working days of receipt – so send the request to the responsible person as soon as possible

Complaints

If people feel that their question has not been answered or it has taken too long to get a response they can complain to the organisation. If this does not resolve the issue, they can then complain to the Information Commissioner's Office[5] (ICO).

Freedom of Information - Good practice

Fig 9 Good practice in freedom of information includes recognising a request

[5] https://ico.org.uk/

Can you recognise a valid FOI request?

Consider the following requests for information. Tick which ones you think are valid FOI requests and which you think are not valid FOI requests, then go to page 46 to check your answers.

Request		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

We rely on records to provide treatment, care and advice to patients and service users.

Fig 10 NHS and care organisations rely on effective record keeping to provide appropriate treatment, care and advice

Consider the following scenario on the value of good record keeping.

A nurse is completing a hospital discharge summary to go to the general practitioner and to the community service that will take over care. The paperwork is missing an NHS number so a check is made against the patient administration system.

There are several patients with the same surname and, unfortunately, the nurse selects the wrong one. The patient she chooses is receiving end of life care and has a ‘do not resuscitate’ notice on her record.

When the discharge summary is received the GP spots the mistake and uploads the summary against the correct record. The community nursing service has a city wide electronic patient record and uploads the summary against the wrong patient. This results in the wrong patient having a ‘do not resuscitate’ marker on their record.

Fortunately on the first visit to the patient, the community nurse asks routine identity checks before medication is issued and the mistake is identified when the patient replies with a different date of birth.

Record keeping - Good practice

Poor quality information presents a risk to patients, service users, staff members and the organisation.

Fig 11 Good practice in record keeping includes making sure that records are accurate, up-to-date and easy to locate

It is vital to ensure that records are:

Accurate

- 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 what 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 and care professional, where necessary, check the information with one or cross reference the information with other records.
- Follow the process in your organisation to report and correct errors.

Up-to-date

- 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 as events occur

- Record information whilst the event, care or otherwise, is still fresh in your mind.

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

- Comply with any procedures that ensure records are stored safely and securely, and can be quickly located when required.

If you are uncertain about any of these, talk to your line manager and improve your understanding.

Revision Question

Which of the following statements are true? Tick true or false for each statement listed below. Then go to page 47 to check your answers.

Options		True	False
A.	Consent is normally needed to use someone's personal information for non-care purposes		
B.	The Data Protection Act prevents information being shared for health and care purposes		
C.	The Freedom of Information Act requires an organisation to respond to requests within 20 working days		
D.	Patients and service users should be given the opportunity to check their own records		

Information security

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

We all need to understand why information security measures are in place, what they aim to prevent happening and ensure they deliver the best protection possible.

Fig 12 Organisations must take measures to ensure their information remains secure

Consider the information security risks in each of the following scenarios.

Scenario A: Angelique (IT Technician)

Can I borrow your ID badge for a few minutes? I need to get into the 'Authorised Area'[6], I've left mine at home and I've only got this temporary pass!

Angelique has left her ID badge at home and has been issued with a temporary pass to the building. She needs to get into the server room so asks to borrow a colleague's ID badge.

What would you do?

Consider the options then look at the feedback on the next page

A.	Lend her the pass	
B.	Tell her you cannot lend her your pass	
C.	Escort her to the area and let her in	

[6] Think about the areas or rooms in your organisation that have restricted access

Feedback

- **Do not lend your ID badge to anyone else:** Not even to close colleagues. You have no control over the security consequences if your badge gets into the wrong hands, but you will be identified by any audit trail as the individual who accessed the system, room or area.
- **Other steps you can take to maintain the physical security of your work premises:** In the workplace wear your ID badge where it can be seen; if safe to do so challenge anyone in a staff/restricted area without a badge; ensure you are not followed through a restricted entrance; don't prop open entrances to secure areas; close windows and lock doors if you are the last to leave.

Scenario B: Lucas (Domestic staff)

"I need to take this confidential waste to the secure disposal point, but I'll leave it here (in the corridor) whilst I check other rooms."

Lucas is supposed to keep the confidential waste with him until he leaves it in the secure disposal point, but he decides to leave it in a busy public corridor whilst he goes to check the waste bins in another room. When he comes back there is confidential waste scattered all over, it seems someone has opened the bag and pulled items out.

If you are moving confidential waste:

- Make sure you do not leave it unattended in unsecure areas.
- Do not overfill the waste bag (or other container).
- Ensure bags (or other container) are securely fastened.
- Follow your organisation's procedure for the secure and confidential disposal of the waste.

Scenario C: Sandra (Care Home Manager)

""I'll leave these notes in the staff office whilst I make a cup of tea for Mr Jones"

Sandra has left the notes in the staff office, which isn't locked and there is no-one else in there. The office is frequently accessed by residents and their visitors. When she gets back the notes are open when she left them closed. Also in the office is information about each resident's location in the home and their current condition.

- **Do not leave people's personal information in unsecured areas**: If you have to leave to do another task, ensure you put items like resident notes in a locked cupboard or lock the door of the office (if possible).

Physical security - Bob's hospital appointment

The previous scenarios looked at some common physical security issues that are encountered every day in health and care. The next scenario takes a look at what happens when the very determined Bob decides to 'visit' his local hospital.

Last week, Bob visited a general practice pretending to be an IT technician. He followed a member of staff into the building and told the receptionist that he needed everyone's details for a software update. Bob then sold these details to other criminals. He doesn't know what they will do with the information, but the money is great.

Doors

Nearly every door Bob encounters in the hospital is open. Even those doors marked as "restricted access" have been propped open to allow for a delivery.

Visitors

Bob is dressed as a doctor and has forged a visitor's pass. He approaches the hospital reception desk and asks for directions to the server room. They are happy to help…his visitor's badge isn't even checked.

Desks

Despite most organisations having strict clear desk policies it was amazing how much information Bob could find in unoccupied office areas. He has a bag of memory sticks and randomly disperses 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

Bob 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 hospital

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

Information security - Good practice

Sometimes, only very simple steps are needed to keep information safe and as protected as possible.

Fig 13 Good practice in information security includes the use of ID badges

Simple steps

- Do shut or lock doors and cabinets as required.
- Do maintain a ‘clear desk’ and ‘clear screen’ policy when away from your desk or device.
- Do wear your building passes or ID if issued.
- Do query the status of strangers (if it is safe to do so), especially if they try to follow people into staff only areas.
- 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 operate, e.g. via social media.
- Do know what an incident is and when and how to report it.

Breaches and incidents

Let's now explore how incidents may arise.

Such incidents typically fall into two categories:

1. A breach of one of the principles of the Data Protection Act and/or confidentiality law and;
2. Technology-related incidents which are generally referred to as 'cyber incidents'.

Fig 14 Incidents typically fall into two categories, namely breaches and cyber incidents

A breach can be caused by a cyber-incident (e.g. disclosure of patient details using social media) but some cyber incidents (e.g. defacing a website) may not involve a breach of information. More information about the different type 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	Other
Technical security failing	
Corruption or inability to recover data	
Unauthorised access or disclosure	
Other	

Examples of breaches and cyber incidents

Your responsibilities

The most commonly reported incidents happen when people don't follow or are not aware of the correct procedures and processes.

- **Make sure you know how to report incidents in your organisation**: If you know or suspect an incident has taken place, report it in line with your organisation's incident reporting procedure. If there is someone who deals with incidents in your organisation, notify them as soon as possible so they can assess how serious the incident is.
- **Make sure you report suspected incidents and any 'near misses' as well**: Lessons can often be learnt from them and they can be closed or withdrawn when the full facts are known.

Incidents - Breaches using the post

Certain procedures can help to reduce the risk of sending personal information through the post.

Fig 15 Sending personal information through the post has risks

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

Miss Broom is waiting to receive information from her social worker. She opens her post one morning and finds as well as her 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 information governance lead for the organisation 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.

What should have happened?

This is a common breach which can be avoided, e.g. by the organisation setting its printers to double-sided printing with automatic stapling of multiple page documents.

This can reduce the risk of someone collecting the letters from the printer and accidentally putting several letters into one envelope.

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.

What can I do?

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

- Make sure all correspondence containing personal information is always addressed to a named person, not to a department, a unit or an organisation – if the information contained in a letter includes more than basic clinical information (e.g. appointment details) consider sending it by recorded or tracked delivery
- Take special care when sending large amounts of personal information (e.g. case notes or care records on paper, encrypted disc or other media) – send these by tracked or recorded post or by NHS courier, to ensure that such information is only seen by the authorised recipient(s) – in some circumstances, obtain a receipt as proof of delivery (e.g. when sending care records to a solicitor)
- Only send case notes and other bulky material in robust approved packaging (never in dustbin sacks, carrier bags or other containers) – don't leave the containers unattended unless securely stored, waiting for collection – make certain that the containers are taken and transported by the approved carrier

Postal checklist

When sending personal information through the post where possible:

- Confirm the name, department and address of the recipient.
- Seal the information in a robust envelope or packaging, checking that only the right information is included.
- Mark the envelope ‘Private and Confidential: To be Opened by the Addressee Only’.
- Check whether you need to send by recorded or tracked delivery or courier.
- Check whether it is necessary to ask the recipient to confirm receipt.

When computer media is being transported between sites, make sure these safeguards are in place:

- Reliable transport or couriers are used.
- Adequate packaging is used to protect the contents from any physical damage likely to arise during transit.
- Additional controls are applied where necessary to protect sensitive information from unauthorised disclosure or modification (e.g. use of locked containers, delivery by hand, tamper-evident packaging, use of encryption).

Reducing incidents - post

Which of the following increases the risk of a breach when sending personal information by post? Tick one option from the statements and then go to page 47 to check your answer.

Options		
A.	Using a trusted postal courier service	
B.	Sending case notes in dustbin sacks	
C.	Sending the package to named person	
D.	Asking the recipient to confirm receipt	

Incidents - Breaches using email

Email is increasingly the preferred vehicle for exchanging information but, as with other forms of information transfer, there are risks.

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

Mr Foster has recently been diagnosed with depression and has joined a support group to help him through his care.

The organisation emails out information to support group members each month. Recently, they have started to receive emails and phone calls from upset individuals about disclosing their names and email addresses to over 500 people.

The organisation undertakes an investigation and finds that a new member of staff had sent out the email. This person was not aware of the difference between the 'CC' and 'BCC' field in the email software and they had put the organisation email address in the 'TO' field and all the members' addresses in the 'CC' field.

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

What should have happened?

The organisation should have had security measures in place to protect personal information, i.e. there should have been a procedure for sending out email and they should have ensured that all staff members were properly trained to do so.

Being a subscriber to the support group is sensitive personal information, so sharing the email addresses could be deemed as disclosure of sensitive personal information.

What can I do?

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 data (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.
- Your organisation will have guidance on sending secure emails. If you need additional guidance about sending email securely using NHSmail, you can access it on the NHSmail portal[7]

[7] http://support.nhs.net/policyandguidance

Reducing incidents - email

After you've answered the following two questions, go to page 47 to check your answers.

Which of the following should you be most cautious about opening emails from? Tick one option from the statements below.

Options		
A.	Unsolicited lenders	
B.	Friends and family	
C.	Colleagues	
D.	Your IT department	

Which of the following increases the risk of a breach when sending personal information by email? Tick one option from the statements below.

Options		
A.	Sending a test email if necessary	
B.	Encrypting the email	
C.	Sending an email to lots of recipients	
D.	Using only the patient's NHS number	

.

Incidents - Breaches using the phone

A request for information over the phone should be treated carefully.

Fig 18 Requests for information over the phone should be treated carefully

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

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

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 got from the practice. At that point, Joe realises he had no proof that the call was from the local hospital.

What should have happened?

The organisation should have had a procedure for providing personal information by telephone. This should make clear how to verify a caller's identity and reason for the request.

What can I do?

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

- Check the caller's identity first by contacting their organisation via a number you already use or by using the number from the phone directory.
- Do not reveal any information unless you are authorised to do so.

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.

Incidents - Breaches using fax

Never send personal information by fax unless it is absolutely necessary.

Some organisations use multi-function printers (photocopiers) to send faxes, this also applies to these devices.

Fig 17 Personal information should not be sent by fax unless absolutely necessary

Consider the following scenario which illustrates how incidents can arise using fax

Rachel works in a care home and is asked to fax some service user information to a local general practice but is in a rush and accidentally gets one of the numbers wrong.

The fax goes off to a local golf club and the manager of the club calls the local newspaper and an embarrassing article about negligence and breach of confidentiality soon follows.

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 eventually results in a fine of £100 000.

What should have happened?

The organisation should have had a procedure for sending faxes and should have ensured that all staff members (especially new staff) followed the procedure.

If Rachel had access to a secure email service she would have been able to send the information to the general practice's NHSmail account.

In future, NHSmail will be rolled out to care homes, such as the one that Rachel works in. Once it is, she will be able to make use of this secure method for sending information, rather than relying on fax, which she currently has no choice but to do.

What can I do?

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

- Leave yourself sufficient time to get everything right.
- Stop and **CHECK** the fax number, then **CHECK** it again.

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.

Reducing incidents

Which of the following should not be used to send personal information unless absolutely necessary? Tick one option from the statements and then go to page 45 to check your answer.

Options		
A.	Post	
B.	Email	
C.	Fax	
D.	Telephone	

Summary

Key points

- Health and care workers have a legal duty to maintain the security and confidentiality of the information we use.
- Information governance aims to protect personal information and make sure it is only used and shared in the right way.
- Information governance is built on confidentiality, data protection, freedom of information, record keeping and information security.
- Information governance incidents may occur as a result of a data breach or a cyber incident.
- Incidents most commonly happen when people don't follow or are not aware of the correct procedures and processes.

Completed Objectives

Having completed this session, you should understand:

- The principles and terminology covered in information governance (IG).
- That health and care personal information is valuable.
- That law and national guidance requires personal information to be protected.
- Your responsibilities when using personal information.

And be able to:

- 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.
- Apply good practice in the workplace.

Resources

You can refer to the following for additional information:

- The NHS Care Record Guarantee[8]. London: NIGB, 2011.
- Department of Health. Information Security Management: NHS Code of Practice[9]. London: DH, 2007.
- Records Management Code of Practice for Health and Social Care 2016[10] IGA, 2016
- Website of the Information Governance Alliance[11]

References

1. Information Commissioner's Office. Chelsea and Westminster Hospital NHS Foundation Trust *monetary penalty notice*[12].
2. Department of Health. Confidentiality: NHS Code of Practice[13]. London: DH, 2003.
3. Information Commissioner's Office[14].
4. Communications Electronics Security Group. Password guidance: simplifying your approach[15].

Related Sessions

- Part 2 of this module for staff who use IT equipment (also known as digital equipment or assets) at work
- Other Data Security modules

---

[8] http://systems.digital.nhs.uk/rasmartcards/documents/crg.pdf

[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200506/Information_Security_Management_-_NHS_Code_of_Practice.pdf

[10] http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

[11] https://digital.nhs.uk/information-governance-alliance

[12] https://ico.org.uk/action-weve-taken/enforcement/chelsea-and-westminster-hospital-nhs-foundation-trust/

[13] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

[14] https://ico.org.uk/

[15] https://www.cesg.gov.uk/guidance/password-guidance-simplifying-your-approach

Answers to workbook questions - Part 1

Characteristics of information

A – If the information includes someone's name and their next hospital appointment, then it will be personal and confidential, e.g. an appointment letter

B – If the information does not directly identify an individual it will be either anonymised or pseudonymised

C – If there are names and addresses included it will be personal and confidential information

D – If the information cannot be linked back to a specific individual by anyone then it is anonymised information

E – If identifying information has been replaced with a code, then this is pseudonymised information

F – If the information directly identifies an individual then it is personal and confidential information

Question		Personal	Confidential	Anonymised	Pseudonymised
A.	Is about an individual's next hospital appointment	**X**	**X**		
B.	The information does not directly identify an individual			**X**	**X**
C.	Might include names and addresses	**X**	**X**		
D.	No-one can link the information back to a particular individual			**X**	
E.	Identifying information will have been replaced with a code				**X**
F.	The information directly identifies particular individuals	**X**	**X**		

Informing people

All of these things can be used to keep people informed about how their information is used.

Options		
A.	Sit down and explain it to them directly	**X**
B.	Direct them to the relevant section on your organisation's website	**X**
C.	Give them a leaflet explaining such matters	**X**
D.	Tell them about their information sharing choices	**X**
E.	Get their consent to use their information where necessary	**X**

Information request

You should find out who is responsible for managing information sharing requests in your organisation

Options		
A.	Provide the information as requested, it's probably alright	
B.	Find out who is responsible for managing information sharing requests in your organisation	**X**
C.	Tell the requestor that they cannot have the information under any circumstances	

Data Protection Act

The Data Protection Act contains a set of rules to help ensure that the use of personal information is fair and lawful, but it does not prevent information being shared for health and care purposes.

Options		
A.	This statement is true	
B.	This statement is false	**X**

Recognising an FOI request

Request		Valid	Not valid	
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

Revision question

Question			Answer
A.	Consent is normally needed to use someone's personal information for non-care purposes	**X**	**True.** There are exceptions to this general rule, but you should not make decisions on whether or not consent is required unless you are qualified to do so
B.	The Data Protection Act prevents information being shared for health and care purposes		**False.** The Act does not prevent information being shared for health and care purposes but contains a set of rules that must be followed in order for the use and sharing of personal information to be lawful
C.	The Freedom of Information Act requires an organisation to respond to requests within 20 working days	**X**	**True.** If an organisation fails to respond within this timeframe, a complaint can be made to the Information Commissioner's Office
D.	Patients and service users should be given the opportunity to check their own records	**X**	**True.** Allowing patients and service users to check the details held about them is one way to confirm that they are accurate, up-to-date and complete

Reducing incidents - post

Options		
A.	Using a trusted postal courier service	
B.	Sending case notes in dustbin sacks	**X**
C.	Sending the package to named person	
D.	Asking the recipient to confirm receipt	

Reducing incidents - email

Options		
A.	Unsolicited lenders	**X**
B.	Friends and family	
C.	Colleagues	
D.	Your IT department	

Options		
A.	Sending a test email if necessary	
B.	Encrypting the email	
C.	Sending an email to lots of recipients	**X**
D.	Using only the patient's NHS number	

Reducing incidents

Options		
A.	Post	
B.	Email	
C.	Fax	**x**
D.	Telephone	

Assessment - Part 1

Attempt **all** of the following **10** questions, and then give the workbook to your IG lead for your answers to be marked

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 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	
E	Individuals cannot 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	
E	General practices are exempt and can choose whether to respond to 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 is an example of an incident? Tick **all options that apply** from the answers listed below.		
A	Some personal information is sent by fax to the wrong recipient	
B	Staff HR files are found in a building vacated by a care organisation	
C	Some paperwork containing personal information is not disposed of securely	
D	Some personal information is revealed in error over the telephone	

Question 10: 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	

You have reached the end of Part 1 of this learning workbook. If you use IT equipment (also known as digital equipment or assets) at work, you should also complete Part 2.

Part 2 - Description

This session explains the most common risks to data security, offers guidance on how to avoid incidents and identifies examples of good practice for those who use IT equipment.

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

Duration: Approx. 30 minutes

Intended audience: Staff who use IT equipment (also known as digital equipment or assets) at work

Learning Objectives

By the end of this session you will understand:

- Understand some basic data security / cyber security terminology.
- Explain your responsibilities when using personal information.
- Identify the most common data security risks
- Identify near misses and incidents and know what to report
- Distinguish between good and poor practice when using personal information

Before commencing this session you should:

- Identify the relevant people in your organisation that are involved in data security such as your information governance lead and IT supplier.
- Where relevant, you should also know the identity of your Caldicott Guardian and/or Senior Information Risk Owner (SIRO).

Introduction

This session aims to highlight how good data security can protect personal information when using computers, mobile phones and other devices.

By the end of this session, you should be more aware of the common data security threats and how important it is that we all play our part in making sure personal information is kept secure and confidential.

Getting it right

Good data security starts at home and in your personal life.

Your attitude towards keeping your own information and possessions secure should be reflected in the way you handle health and care information, whether it is in digital or paper records.

Getting it right - Overview

Your network

You should know who has access to your home Wi-Fi network. When you go home today check that a password is set up to control who can access your network.

You shouldn't give your Wi-Fi password to your neighbour or a stranger as they could use your internet connection, leaving you liable for any illegal activities they might engage in.

This should also apply to work-related systems and networks – **never** give out your work password to anyone.

If you would like to find out more about securing your personal devices check out Get Safe Online[16].

Your money

Online banking is one area that uses technology to make transactions much easier - if someone stole from your bank account, you would immediately be aware that something was wrong.

[16] https://www.getsafeonline.org/

Criminals have become sophisticated in their methods to find your password details and, therefore, an easy route into your account - **never** give out your password to anyone.

This advice also applies to work-related systems - especially those where you record personal information about patients, service users or staff.

Physical security

When you leave home, you lock the doors and windows so that a burglar doesn't steal your possessions.

Most workplaces have control systems allowing you to only have access to areas that you need - access control systems are designed to keep an organisation's infrastructure secure - some of this infrastructure is critical to operations.

Where access controls are in place, remember to close doors and, in certain areas of buildings, ask for ID where required - this is particularly important if you spot someone in an area where they shouldn't be, e.g. the ICT department or near networking equipment.

Getting it right - Setting passwords

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

Unique passwords

It's easy to have one or two familiar passwords, only changing one or two digits when required, for all of your online accounts. However, this makes it easier for someone to control your digital life, having only gained access to a single source.

This could include

- Your bank account.
- Your Facebook account.
- Your WhatsApp account.
- Your work network login.
- Your work or personal email account.
- Your online government accounts, e.g. your tax, passport and driving licence records.

Once someone has control of your email account they can reset passwords on many of your other online accounts, locking you out of them.

Strong passwords

Using strong passwords on all your accounts is an excellent first line of defence. It means that to guess your password would take a long time.

When you are creating a password, it should:

- Use **at least** three random words - substitute letters with numbers or symbols to make them non-dictionary words.
- Be a **minimum** of 8 characters long, and the recommendation is that they are at least 15 characters long.
- Not contain your user name, real name, or company name
- Be significantly different from previous passwords
- Remember you should have a number of passwords and change them regularly

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

Character types

- A strong password should contain a mix of character types:
- Upper case letters (e.g. A, B, C)
- Lower case letters (e.g. a, b, c)
- Numbers (e.g. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
- Symbols (e.g. ‘ ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; “ < > , . ? /)

An example strong password would be: !Rainb0w3D4$h4COv3r!

It would take a hacker using a powerful computer 552 quadrillion years to crack this example. Using the ‘three random words’ techniques, you can create passwords that are relatively simple to remember.

Warning: Do not use this actual example as your password!

Helpful resources

A number of online resources can help you create a new password (e.g. Strong Password Generator[17]).

In addition, you can use a secure password manager/logger for your personal devices (e.g. Dashlane[18], Lastpass[19], KeePass[20])

Antivirus software usually comes with password storage tools depending on which package you buy.

Getting it right - Staying safe online

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

Locking devices

STOP, **THINK** and **CHECK** before you leave a device unattended

Lock your device as soon as you leave it. ALL mobile phones, laptops, computers and tablets, whether work provided 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 applies to corporate mobile devices - activate the lock function so that a password or code is needed to unlock them.

Opening emails

STOP, **THINK** and **CHECK** before opening an email. It could be a fake phishing email.

Remember, this is another simple way for criminals to install malware on a device or fraudulently obtain your login details.

Does the email look genuine, or is it social engineering being used to make you act quickly, so that sensitive login information can be reviewed?

---

[17] https://strongpasswordgenerator.com/
[18] https://www.dashlane.com
[19] https://lastpass.com
[20] http://keepass.info

If you do suspect phishing, take these steps:

- Do not reply.
- Put the email in your junk or spam folder.
- Ensure suspicious email domains are blocked and these emails are sent to the spam or junk folder.
- In many cases, your organisation will have a process for dealing with spam. If you receive these emails persistently, inform your local ICT department or provider. More information on how to report suspicious emails and websites can be found on GOV.UK[21]
- Services can be used to check if URLs are safe - however, only use a reputable service, (e.g. VirusTotal[22]) as there some fakes.

Unauthorised devices

STOP, **THINK** and **CHECK** before plugging a USB drive into your computer.

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.

Scan USB devices before using them, to ensure they are safe to use. A USB device is technically a small computer. If you plug it into an untrusted computer that has malicious software on it, this could be transferred to the USB and then onto any other devices you plug it into.

Checking web links

STOP, **THINK** and **CHECK** before clicking on web links.

Even if you think you've entered a genuine site via an online search, you must always make sure you are aware of what and where the website is.

Look out for warnings from your web browser about security when entering a site.

Some web browsers provide an indication of the trustworthiness of websites - this means the reputability of the website has been checked.

---

[21] https://www.gov.uk/report-suspicious-emails-websites-phishing
[22] https://www.virustotal.com/

Untrusted websites

STOP, **THINK** and **CHECK** 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, which has been made to look genuine.

A browser may display a red padlock for internal sites if certificates haven't been stored properly or the site added to trusted sites. If you see a red padlock on an internal site, contact your IT department or provider. Your browser may display a red lock icon or a warning message stating 'Your connection is not private'.

Getting it right - Mobile devices

Most of us now have at least one 'digital asset' - a laptop, tablet, mobile or other device that stores and processes information and can be connected to devices and networks.

If you use a digital asset at work, comply with your organisation's policies and procedures and follow these simple 'dos' and 'don'ts'

Digital 'dos'

- 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 anti-virus software if your digital asset prompts you to do so.
- Do keep regular backups of the data stored on digital assets and store appropriately according to your organisation's policies.
- Do report immediately any lost or stolen digital asset to the police and via your organisation's incident management procedure (failure to report a stolen mobile phone could result in significant charges).
- Do ensure that digital assets and passes are handed in if you are leaving employment.

Digital ‘don’ts’

- Don’t use your own digital assets for business purposes unless you have been properly authorised.
- Don’t use digital assets provided by your organisation outside business premises unless you are authorised to do so.
- Don’t use work-provided digital assets for personal use (e.g. social media, personal web browsing, etc) unless you are authorised to do so.
- Don’t connect your work-provided digital asset to unknown or untrusted networks, e.g. 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 (e.g. by email, on a USB stick) off site without authorisation.
- Don’t leave digital assets where a thief can easily steal them, e.g. visible or unattended in your car or a public place.
- Don’t install unauthorised software or download software or data from the Internet.
- Don’t disable the anti-virus protection software.

Cyber Incidents

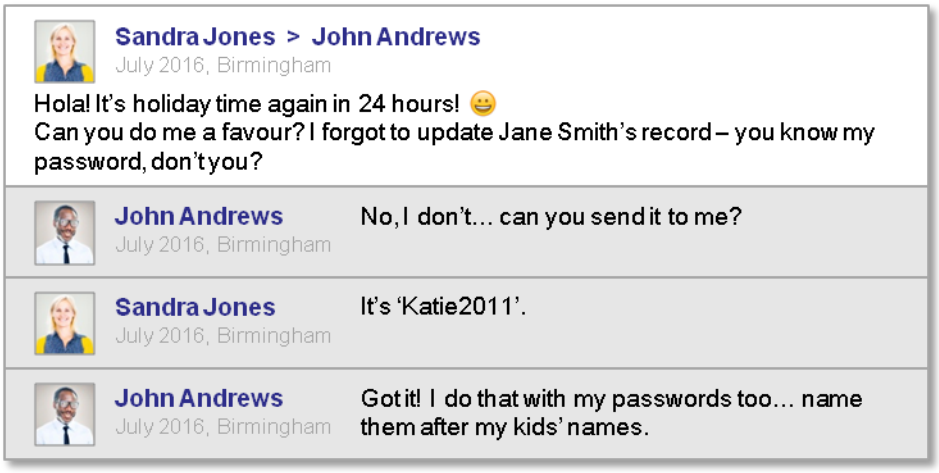
Using social media

Bob the fraudster likes to stake out organisations before stealing from them. He does this to find out about their weaknesses or vulnerabilities.

To reduce the risk of being targeted by cyber-criminals like Bob, limit the amount of information you post about yourself or your job on social media. You may include sensitive information without even realising.

To illustrate, consider these social media posts between a mental health worker and her colleagues.


Sandra Jones
March 2016, Birmingham
The mental health team is really on fire today!
Sandra Jones
April 2016, Birmingham
It's office move day today, so we're having to use these stupid passes and door entry codes everywhere.
Sandra Jones
April 2016, Birmingham
The amount of codes I have to remember these days is crazy! Mine are all the same anyway.
Sandra Jones
May 2016, Birmingham
Having to sort out all this funding today... we've just been awarded £1m to cut our waiting times. So, guess what? I can sign off up to £50,000 now. How senior am I?
Sandra Jones > John Andrews
June 2016, Birmingham
I can't get in the office! Can you send me your door code?
John Andrews
June 2016, Birmingham
Sure... it's 12345.



In this example, Bob the fraudster was able to:

- 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 first time around, Bob will gain vital intelligence about how your processes work.

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

Cyber incidents - Question1

Which of the following best describes someone who attempts to misuse or steal health and care information? Tick one of the options from the list below, then go to page 71 to check your answer.

Options		
A.	A teenager living at home with parents	
B.	A disgruntled former employee	
C.	A political activist	
D.	There is no typical profile for someone like this	

Cyber incidents - Question 2

Which of the following best describes why someone would want to steal patient or service records? Tick one of the options from the list below, then go to page 71 to check your answer.

Options		
A.	To create fake online profiles	
B.	To extort money from patients or service users	
C.	To sell the data for financial gain	
D.	To steal people's identity	
E.	To dupe patients into buying bogus cures	
F.	To find out more information about relatives	
G.	All of the above	

Cyber incidents - Question 3

Consider the following statement. “You only need to be aware of data security at work”. Tick one of the options from the list below, then go to page 71 to check your answer.

Options		
A.	This statement is true	
B.	This statement is false	

Data security risks

Data security is an increasingly serious issue for all organisations. Preventing a successful attack, whilst keeping systems open and easy to use is a big challenge. Hence, a 100% secure environment can never be achieved.

In this section, we will focus on:

- Social engineering
- Phishing
- Malware
- Reporting incidents

Social engineering

Hackers have a range of digital tools at their fingertips. They might also try to employ confidence tricks or resort to the interception or theft of devices or documents.

This includes digital or physical, such as printed documents or mobile phones, in order to gain further access to more protected systems.

Phishing

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

Criminals use phishing emails and websites to scam thousands of people every week. They are just waiting for you to click their fake links to sites or attachments in order to steal your sensitive data.

Phishing emails

The aim of phishing emails is to force users to make a mistake, e.g. 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 through a macro* command in a document.

STOP: Do not install any new software unless you are advised to do so by your IT department.

THINK: Is someone trying to extract or extort information from you?

CHECK: If you are unsure or think this is happening to you then you need to check it out with your colleagues, your manager or IT department or provider.

***Macros**

Macros are a series of actions that a programme such as Microsoft Excel may perform to work out some formulas. Your computer will disable these by default as hackers can programme these macros to install malware.

STOP, **THINK** and **CHECK** - before clicking on 'enable macros' or 'edit document' that the source of the file can be trusted.

Data security risks - Question 1

Which of the following increases the risk of a breach when sending personal information by email? Tick one of the options from the list below, then go to page 71 to check your answer.

Options		
A.	Sending a test email if necessary	
B.	Encrypting the email	
C.	Sending an email to lots of recipients	
D.	Using only the patient's /service user's NHS number	

Email servers

In rare instances, an organisation's email server can be hacked into and taken over by criminals, locking out IT staff. Criminals may then have the ability to send emails from genuine email accounts in your organisation.

Checking that an email has come from a genuine account becomes redundant, as the email clearly has come from an official account. Once an email server has been hacked, messages can be delivered to every address that has ever sent, or received, an email from this server - under the veil of a genuine email address.

If you receive a request from a colleague asking for login details or sensitive financial or patient/service user information, you should **STOP**, **THINK** and **CHECK** with your colleague over the phone.

Never give out your login details to anyone, even if they claim to be from your IT department

Malware

Hackers utilise many different tools and methods to gain illegal access to information.

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

To protect yourself from these types of threat, ensure that you have up-to-date antivirus software installed

Has malware been installed on my computer

Be alert to the following signs:

Slow computers: Some staff presume that work computers do not function as well as personal devices. If a computer is working slowly, this may be a sign that it has a virus or malware installed. If your work computer is acting strangely in any way, you should report this to your IT department or provider.

Malfunctioning software: If you have antivirus or security updates that are telling you that there is a problem you MUST report it to your IT department or provider. It is

important that we all remain vigilant to system warning messages and actually read what they say.

Common types of malware include viruses, worms, Trojans and bots.

Reporting incidents

You might recall from Part 1 of this course (see page 32) that incidents typically fall into two categories:

1. A breach of one of the principles of the Data Protection Act and/or confidentiality law and;
2. Technology-related incidents which are generally referred to as 'cyber incidents'.

Also that, a breach can be caused by a cyber-incident (e.g. disclosure of patient details using social media) but some cyber incidents (e.g. defacing a website) may not involve a breach of information. This table below contains a reminder of what you must report.

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	Other
Technical security failing	
Corruption or inability to recover data	
Unauthorised access or disclosure	
Other	

Your responsibilities

Remember

- **Make sure you know how to report incidents in your organisation**: If you know or suspect an incident has taken place, report it in line with your organisation's incident reporting procedure. If there is someone who deals with incidents in your organisation, notify them as soon as possible so they can assess how serious the incident is.

- **Make sure you report suspected incidents and any 'near misses' as well**: Lessons can often be learnt from them and they can be closed or withdrawn when the full facts are known.

Data security risks - Question 2

Which of the following are tell-tale signs of a phishing email? Tick one or more of the options from the list below, then go to page 71 to check your answer.

Options		
A.	The sender using your name in an email	
B.	Suspicious links to unencrypted websites	
C.	Requests for personal of confidential information	
D.	Email attachments or calendar invites from unknown senders	
E.	Excellent spelling and punctuation	

Data security risks - Question 3

Which of the following should you do immediately if you believe you have received a phishing email? Tick one or more of the options from the list below, then go to page 71 to check your answer.

Options		
A.	Report it to your Helpdesk	
B.	Click one of the links in it to see if it goes to a valid website	
C.	Report it in line with your IT department/provider's procedures	
D.	Forward the email to a friend to check whether it is a phishing email	

Data security risks - Question 4

Which of the following should you be most cautious about opening emails from? Tick one or more of the options from the list below, then go to page 71 to check your answer.

Options		
A.	Unsolicited senders	
B.	Friends and family	
C.	Your colleagues	
D.	Your IT department/provider	

Summary

Key points

- Patients and service users trust us to look after and respect their information at all times.
- Health and care information is valuable and some people may want to misuse it for a variety of reasons.
- Good data security can help you to protect health and care information from those who wish to misuse it.
- Data security risks include social engineering, phishing, malware and physical security risks.
- Data incidents can happen with the post, fax, telephone and email.
- Strong passwords, staying safe online and careful use of digital assets can help to promote good data security.

Completed Objectives

Having completed this session, you should be able to:

- Understand some basic data security / cyber security terminology.
- Explain your responsibilities when using personal information.
- Identify the most common data security risks.

- Identify near misses and incidents and know what to report.
- Distinguish between good and poor practice when using personal information.

Resources

You can refer to the following for additional information:

- The NHS Care Record Guarantee[23]. London: NIGB, 2011.
- Department of Health. Information Security Management: NHS Code of Practice[24]. London: DH, 2007.
- Records Management Code of Practice for Health and Social Care 2016[25] IGA, 2016
- Website of the Information Governance Alliance[26]

References

- VirusTotal[27]
- NHS Digital. Sending secure email[28]
- Strong Password Generator[29]
- Dashlane[30]
- LastPass[31]
- KeePass[32]
- GOV.UK. Avoid and report internet scams and phishing[33]
- Communications Electronics Security Group. Password guidance: simplifying your approach[34].

[23] http://systems.digital.nhs.uk/rasmartcards/documents/crg.pdf
[24] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200506/Information_Security_Management_-_NHS_Code_of_Practice.pdf
[25] http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf
[26] https://digital.nhs.uk/information-governance-alliance
[27] https://www.virustotal.com/
[28] http://systems.digital.nhs.uk/nhsmail/secure/index_html
[29] https://strongpasswordgenerator.com/
[30] https://www.dashlane.com/
[31] https://lastpass.com/
[32] http://keepass.info/
[33] https://www.gov.uk/report-suspicious-emails-websites-phishing
[34] https://www.cesg.gov.uk/guidance/password-guidance-simplifying-your-approach

Related Sessions

- **Data Security Level 2** – A course designed for those managing IT and IG functions on key cyber security terms and the National Data Guardian (NDG) standards.
- **Data Security Level 3** - A course designed for those leading IT and IG functions at a Board level to gain an understanding of key cyber security terms and NDG standards.

Answers to workbook questions - Part 2

Cyber incidents - Question 1

Options		
A.	A teenager living at home with parents	
B.	A disgruntled former employee	
C.	A political activist	
D.	There is no typical profile for someone like this	**X**

Cyber incidents - Question 2

Options		
A.	To create fake online profiles	
B.	To extort money from patients or service users	
C.	To sell the data for financial gain	
D.	To steal people's identity	
E.	To dupe patients into buying bogus cures	
F.	To find out more information about relatives	
G.	All of the above	**X**

Cyber incidents - Question 3

Options		
A.	This statement is true	
B.	This statement is false	**X**

Data security risks - Question 1

Options		
A.	Sending a test email if necessary	
B.	Encrypting the email	
C.	Sending an email to lots of recipients	**X**
D.	Using only the patient's /service user's NHS number	

Data security risks - Question 2

Options		
A.	The sender using your name in an email	
B.	Suspicious links to unencrypted websites	**X**
C.	Requests for personal of confidential information	**X**
D.	Email attachments or calendar invites from unknown senders	**X**
E.	Excellent spelling and punctuation	

Data security risks - Question 3

Options		
A.	Report it to your Helpdesk	**X**
B.	Click one of the links in it to see if it goes to a valid website	
C.	Report it in line with your IT department/provider's procedures	**X**
D.	Forward the email to a friend to check whether it is a phishing email	

Data security risks - Question 4

Options		
A.	Unsolicited senders	**X**
B.	Friends and family	
C.	Your colleagues	
D.	Your IT department/provider	

Assessment - Part 2

Attempt **all** of the following **12** questions, and then give the workbook to your IG lead for your answers to be marked

Question 1: 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 2: Which of the following represents a secure way of working? Tick **one option** from the answers listed below.		
A	Using WhatsApp to send some x-ray images	
B	Using your partner's work USB to transfer some files from your work laptop	
C	Using your personal email account to send work home	
D	Using your work laptop to check your NHSmail2 account at home	

Question 3: Which of the following is the best course of action if your system starts malfunctioning or running slowly? Tick **one option** from the answers listed below.		
A	Do nothing…systems are often slow and you have no reason to believe there is a security risk	
B	Monitor the problem…if it carries on, speak to your IT department /provider	
C	Report the problem…it's best to assume this is unexpected behaviour	

Question 4: 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 5: Consider the following statement: "It is important to lock your computer or work-provided digital asset when you are not using it." Tick **one option** from the answers listed below.		
A	A. This statement is true	
B	A. This statement is false	

Question 6: 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 7: Which of the following represents an example of a cyber incident? Tick **one option** from the answers listed below.		
A	Some personal information is sent by fax to the wrong recipient	
B	Staff HR files are found in a building vacated by a care organisation	
C	A social worker receives a phishing email requesting personal information	
D	Some paperwork containing personal information is not disposed of securely	
E	Some personal information is revealed in error over the telephone	

.

Question 8: 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 9: 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 10: Consider the following statement. “There is no need to report an incident so long as it was a ‘near miss’.” Tick **one option** from the answers listed below.		
A	This statement is true	
B	This statement is false	

Question 11: Which of the following statements best describes how to respond to a ‘cyber incident’? Tick **one option** from the answers listed below.		
A	All cyber incidents should be reported	
B	A cyber incident should be reported only if it results in personal information being revealed	
C	A cyber incident should be reported only if it results in personal information being corrupted	
D	A cyber incident should be reported only if it results in a denial of service	
E	There is no need to report a cyber incident	

Question 12: 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 learning workbook.