e-Learning for Healthcare

NHS Digital

Data Security Awareness Level 1

Information and technology
for better health and care

Welcome

- NHS Digital delivers information and technology for better health and care.
- We have developed this presentation to:
  - Help health and care staff use and share information in a lawful and secure way.
  - Promote good practice that should be adapted for your working environment.

Description

- Your organisation is required to provide annual training on topics such as:
  - The Data Protection Act
  - The Freedom of Information Act
  - The adoption of technology – building and maintaining public trust in how we use and share information
  - Information security policy and procedure
- This presentation provides an overview and guidance and good practice on the above topics.
- Author: NHS Digital (Data Security Centre and External IG Delivery)
- Duration: Approx. 1 hour

Learning Objectives

By the end of this session you will understand:

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

And be able to:

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

Why is Data Security important in Health and Care?

- Data Security has always been important.
- More complex now technology is so central to delivery of health and care.
- Use technology so does not pose unacceptable risk to organisation or patients / service users.
- We all have a duty to protect people's information in a safe and secure manner.

Technology enables us to deliver a better quality of care

Information can be shared more quickly

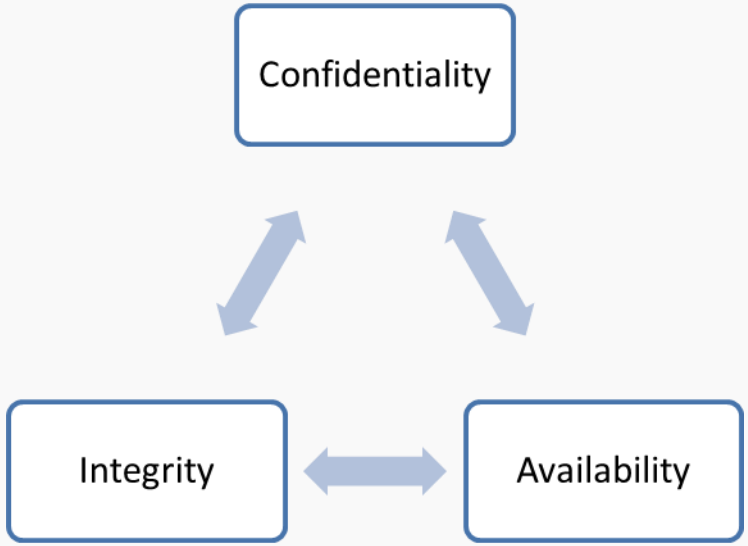
Powerful analysis can be performed to improve the future of care

Safe data, safe care

- Good information underpins good care. Patient and service user safety is supported by:
  - Confidentiality
  - Integrity, and
  - Accessibility.
- Patients / service users must feel assured that their information is used appropriately.
- You can help with this by following the good practice set out in this presentation.

Confidentiality, Integrity, Availability

- **Confidentiality** is about privacy and ensuring information is only accessible to those with a proven need to see it.
- **Integrity** is about information stored in a database being consistent and un-modified.
- **Availability** is about information being there when it's needed to support care.



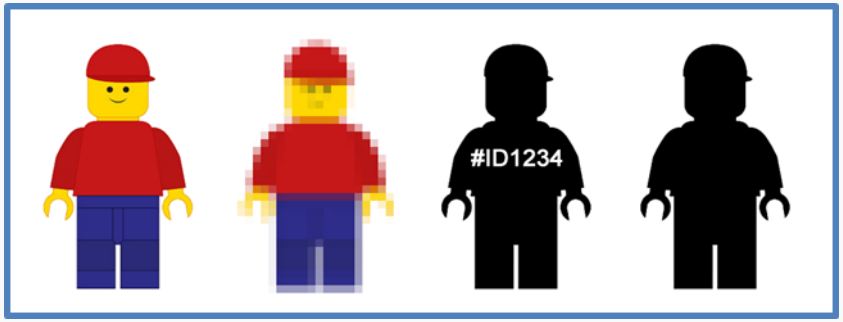
Summary

- This section introduced:
  - The concepts of confidentiality, integrity and availability, and
  - Why data security is important to patient and service user care.
- The next section looks in more detail at the threats to patient and service user information, and the legal obligations of all staff in health and care when accessing patient information.

Information and the Law

- We will now look in more detail at managing patient and service user information in health and care. This section covers:
  1. Confidentiality - good practice.
  2. The Data Protection Act, including the rights of patients and service users.
  3. The Freedom of Information Act, including how to comply.
  4. Good record keeping.

Types of information



- In health and care settings, there are various types of personal information.
- It is important to be able to identify these different types of information so that they can be appropriately protected when they are used and shared.

Types of information

- In health and care settings, you might see:
  - Confidential information.
  - Sensitive information.
  - Personal information.
  - Pseudonymised information
  - Anonymised information.
- These different types of information are defined in the notes section below.

The Value of Information

- Health and care information is valuable.
- Poor security can cause personal, social and reputational damage.
- Some of the common ways that information is lost:

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

Common law duty of confidentiality

- Information that individuals disclose in confidence should not be used or shared further without a lawful reason: The lawful reasons are:
  - The consent of the individual.
  - Where there is a legal reason to disclose information.
  - Where there is a public interest justification.
- A decision to disclose without consent should be made by senior staff.
- Check what the procedure is in your organisation.

The Caldicott Principles

- **Principle 1**: Do you have a justified purpose for using confidential information?
- **Principle 2**: Is it absolutely necessary to do so?
- **Principle 3**: Are you using the minimum information required?
- **Principle 4**: Are you allowing access to this information on a strict need-to-know basis only?
- **Principle 5**: Do you understand your responsibility and duty to the subject with regards to keeping their information secure and confidential?
- **Principle 6**: Do you understand the law and are you complying with the law before handling the confidential information?
- **Principle 7**: Do you understand that the duty to share information can be as important as the duty to protect confidentiality?

Confidentiality – Good practice

- We all have a legal duty to respect the privacy and to use personal information appropriately.
- The main aspects of confidentiality good practice are:
  - Informing people
  - Sharing information for care
  - Sharing information for non-care

Confidentiality - Informing People

- You should inform patients and service users that you are accessing and using their information.

Explain

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

Give choice

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

Meet expectations

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

- You don't need to obtain consent every time you use information for the same purpose, providing you have previously informed the individual.

Confidentiality - Sharing information for care

- Sharing information with the right people can be just as important as not disclosing to the wrong person.
- Note the **duty to share** for care where the right conditions are met.

Check

Check that the individual understands what information will be shared and has no concerns.

Best practices

Ensure that the data protection, record keeping and security best practices covered later in this presentation are met.

Respect objections

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

Confidentiality - Sharing information for non-care

- In many cases - obtain consent
- If there is a risk of immediate harm:
  - Share first.
  - Then inform the person responsible for IG as soon as possible.

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

Data Protection

Rights under the Act include:

- To be told what personal information is being used for.
- To see and have a copy of your personal information.
- To have objections to processing considered in some circumstances.

Rights of Individuals

- Individuals have rights in relation to their information including:
  - Make subject access requests.
  - Have inaccuracies corrected.
  - Have information erased (where it has not been relied upon to provide health or care).
  - Object to direct marketing.
  - Restrict the processing of their information.
- Patient / service users might be able to view their record online – online access should not reveal information that they do not already know relating to 3rd parties.

Data Protection - Good Practice 1

- Follow your organisation’s policies and procedures.
- No surprises - handle people’s information as you’d expect others to handle your personal information.
- Be open, honest and clear about:
  - Why you need personal information.
  - What you intend to do with it.
  - Who you may share it with.
  - How the individual can obtain a copy.

Data Protection - Good Practice 2

- **Remember** - patients and service users have a right to see information recorded about them. So make sure you:
  - Record clearly so that others can rely on your entries.
  - Be accurate and keep information up-to-date.
- Follow your organisation's rules when disposing of personal information.
- Note the impact of the General Data Protection Regulation (GDPR).

The Freedom of Information Act 2000

The Act allows anyone from anywhere in the world to make a **written** request for information held by a public body.

The Act only applies to information that already exists in a recorded form.

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

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

Handling FOI requests

- FOI requests should be handled by trained staff.
- Normally, you should not try to handle a request yourself.
- If you are not sure whether a request is BAU or FOI, ask.
- If your organisation is subject to the Act:
  - Make sure you know who is responsible for managing requests.
  - Send any FOI requests to the person responsible immediately.

Activity - Can you recognise a valid request?

Identify which ones you think are valid FOI requests and which you think are not valid FOI requests	
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?

Activity - Can you recognise a valid request?

Identify which ones you think are valid FOI requests and which you think are not valid FOI requests		Valid or not valid
A.	Please send me a copy of my social care record	Not valid
B.	How many GPs work in the practice?	Valid
C.	When's my daughter's next appointment?	Not valid
D.	How much did the Trust spend on rail travel last year?	Valid
E.	How many staff have passed their IG training?	Valid
F.	What services are being considered for closure in the next year?	Valid

Record keeping - Good practice

Poor quality information presents a risk to patients, service users, staff members and the organisation. It is vital that records are:

- **Accurate and up to date.**
  - Know ‘what and why’ needs recording in the correct system/record.
  - Check the information.
  - Report errors.
- **Recorded and complete.**
  - At the time events occur.
  - Include NHS number.
  - Don't create duplicate records.

Seek help if you are uncertain.

Scenario

- Bill is seeking treatment for depression and has not told his work colleagues.
- Due to a data entry error, the clinic contacts him at work rather than on his personal number.
- His colleague answers, and is mistaken for Bill.
- The colleague discovers Bill's condition and proceeds to tell other colleagues.
- Embarrassed, Bill resigns and makes a formal complaint to the clinic.

This scenario shows the importance of:

- Entering information accurately into the correct systems.
- Verifying identity before disclosing confidential information.

Summary

- We all have a responsibility to use information lawfully.
- Sharing information can improve speed and quality of service.
- Make sure it is shared in a secure way.
- Gain consent where necessary.
- Allow individuals to check the accuracy of information held about them.
- If you are unsure - seek advice from those who are responsible for IG in your organisation.

Avoiding threats to data security

This section looks in more detail at potential threats to the security of information in the workplace.
You will learn about:

- Social engineering.
- Email phishing and malware.
- Good practice for protecting information.

Social engineering

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

On the phone: A social engineer might call and pretend to be a fellow employee or a trusted outside authority (such as law enforcement or an auditor).

In the office: "Can you hold the door for me? I don't have my key/access card on me." How often have you heard that in your building? While the person asking may not seem suspicious, this is a very common tactic used by social engineers.

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

The fake ICT Department

- Criminals have set up call centres that make calls to health organisations or social care providers.
- They ask for your username, password, email address or other details about where you work.
- They may ask you to click on a malicious web or email link.
- Your ICT department or provider will **not** need to ask these types of questions.

Social Engineering - what you can do

- Always be vigilant:
  - When using the phone,
  - Receiving unsolicited emails,
  - Using social media, or
  - Walking around your place of work.
- If it's **safe** to do so:
  - Challenge suspicious behaviour, and
  - Request proof of identification.

Email phishing and malware

Email though efficient has **risks**:

- Criminals use email attachments and links to trick people into providing information.
- Email attachments may be executable files that contain malicious software (malware).

This is known as **phishing** and the emails aim to force you to make a mistake.

- Never give your login details to anyone.
- If you receive an email requesting sensitive information that looks as though its from a colleague - double check by phoning the colleague.
- Do not open links or attachments in unsolicited emails.

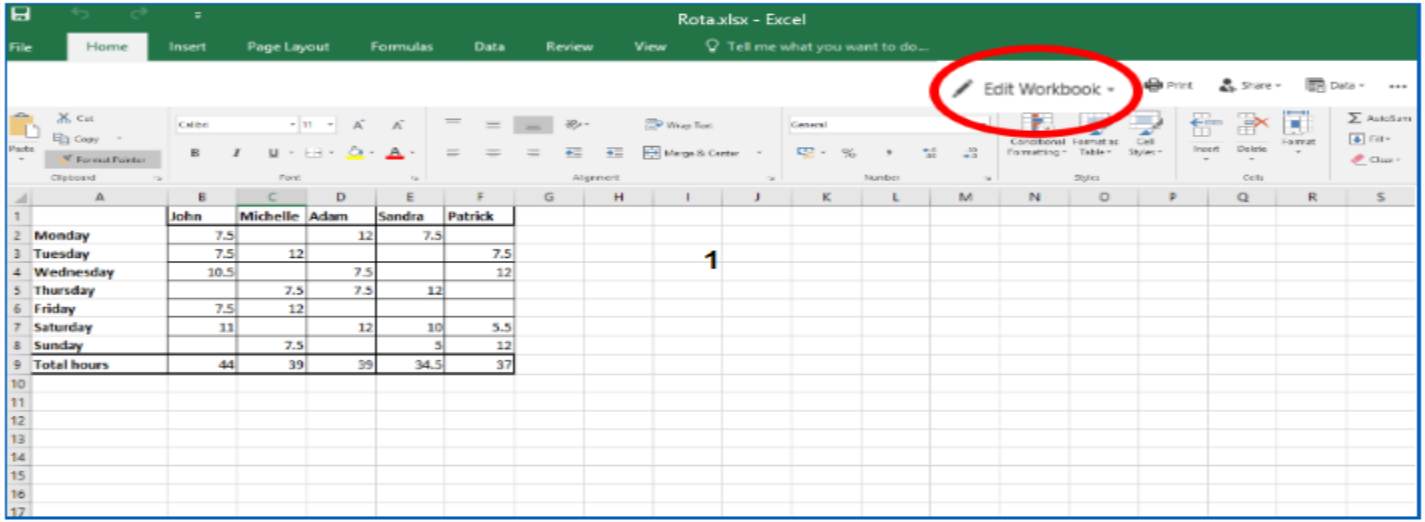
Report suspicious emails to your ICT department or provider.

Phishing - what to do

- Be vigilant:
  - Do not install any new software unless authorised.
  - **Think** - Is someone trying to extract or extort information?
  - Discuss issues with your manager and ICT department/provider.
- If you do identify a phishing email, take these steps:
  - Do not reply.
  - Select the email, right-click it and mark it as junk.
  - Block suspicious email domains.
  - Inform your local ICT department or provider - your organisation is likely to have a process for dealing with spam.

Macros

- Macros are a series of actions that a program such as Microsoft Excel may perform to work out some formulas.



	A	B	C	D	E	F
1		John	Michelle	Adam	Sandra	Patrick
2	Monday	7.5		12	7.5	
3	Tuesday	7.5	12			7.5
4	Wednesday	10.5		7.5		12
5	Thursday		7.5	7.5	12	
6	Friday	7.5	12			
7	Saturday	11		12	10	5.5
8	Sunday		7.5		5	12
9	Total hours	44	39	39	34.5	37

Always be vigilant - do you trust the source of the document?

Malware

- Malicious software (malware) can:
  - Be on your computer and evade detection.
  - Make your computer run slowly or perform in unusual ways.
- Your ICT department or provider will:
  - Ensure that you have up-to-date antivirus software installed.
  - Assist if you suspect your computer is not performing as it normally does.

Good practice - Setting passwords

- Use strong passwords on all your devices to prevent unauthorised access - use different passwords for each account.
- Follow simple guidelines to create strong passwords, e.g.
- The National Cyber Security Centre (NCSC) guidance on:
  - Setting secure passwords: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0.
  - Using a password manager: https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers.

Good Practice - Locking Devices

- Lock your device as soon as you stop using it.
- Set passcodes on mobile phones, laptops, PCs and tablets.
- If you see a colleague's device open and unlocked, lock it for them and gently remind them to do so in future.
- On corporate mobile devices - activate the lock function.
- Tip: select the Windows Key + L on your keyboard to quickly lock your laptop or PC.

Good practice - Removable drives

- Do not use unauthorised USB drives.
- Do not plug in any non-approved devices to charge via a USB cable.
- Scan USB drives before use.
- Ask your ICT department or provider if you are unsure.

Good practice - Untrusted websites

- Be vigilant when you visit a website that is declared "untrusted".
- If a web browser states that you are about to enter an untrusted site, be very careful – it could be a fake phishing website that has been made to look genuine.
- A browser may display a red padlock or a warning message stating ‘Your connection is not private’."

Good practice - Mobile devices

Digital Do’s

- Read, understand and comply with your organisation's policy and procedures.
- Seek advice from your line manager if any aspects of the policy or procedures are unclear.
- Store your digital assets securely when not in use.
- Update antivirus software if your digital asset prompts you to do so.
- Keep regular backups of the data stored on digital assets – store appropriately, according to your organisation’s policies.
- Report any lost or stolen digital asset to the police immediately.
- Follow your organisation’s incident management procedure.
- Ensure that digital assets and passes are handed back if you are leaving the organisation.

Good practice - Mobile devices

Digital Don’ts

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

Good practice - Disposal of confidential information

- Take special care to securely dispose of:
  - Paper records that contain confidential information
  - Desktop computers
  - Servers
  - Multifunction devices (e.g. Printers/Photocopiers)
  - Laptops, tablet computers and electronic notebooks
  - Mobile telephones
  - Digital recorders
  - Cameras
  - USB devices
  - DVDs, CDs and other portable devices and removable media.
- Follow your organisation’s processes for secure disposal.

Good practice - Clear desks

- Follow your organisation’s clear desk policy.
- Do not leave information in unsecure locations.
- Having a clear desk means reduced potential for leaving sensitive information unattended, reducing the risk of a breach.

Summary

- In this section you have learnt about different types of data security threat, how to spot them, and what to do.
- The learning also covered good practice in the workplace.
- The last section covers what to do if you identify that a security incident or breach has occurred.

Breaches and incidents

- The section covers:
  - Identifying breaches and incidents
  - Reporting breaches and incidents
  - Avoiding breaches and incidents
  - Everyday scenarios where information can be lost.

- Covers two categories:
  - A breach of one of the principles of the Data Protection Act 1998 and/or confidentiality law.
  - Technology-related incidents.

Different types of incident

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

Most reported breaches in health and care

- From the Information Commissioner trend reports about breaches and incidents:
  - Faxes that are sent to the wrong number or misplaced.
  - Lost or stolen paperwork.
  - Failure to adhere to principle 7 of the Data Protection Act 1998.

Incidents using technology

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

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

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

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

Consequences of breaches and incidents

- How can an important decision about a person's care be made if:
  - Their record was no longer available, was wrong or incomplete; or
  - Someone had tampered with it.
- By now you should understand why security measures are in place.
- We all need to help ensure that information is protected in the best way possible.

Reporting incidents

Postal breach

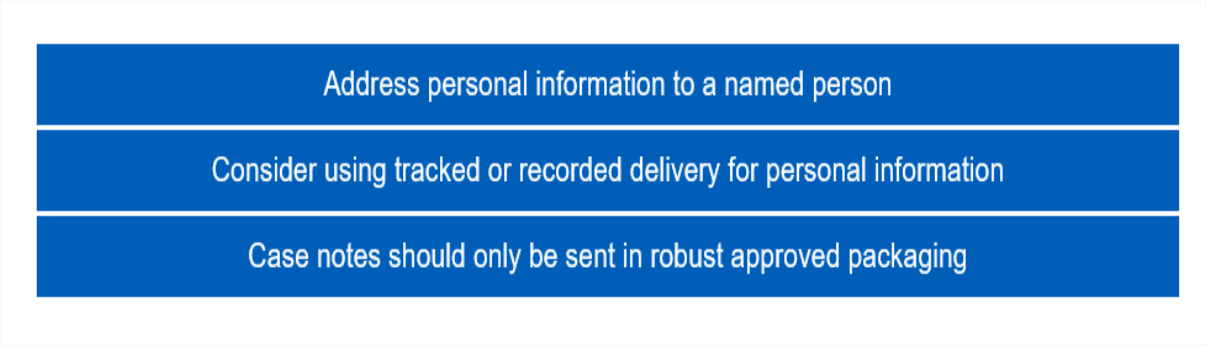
The situation - Miss Broom is waiting to receive information from her social worker. She opens her post one morning and finds that, as well as her own letter, the envelope contains two further letters addressed to other people.

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

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

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

Postal checklist



Email breach

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

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

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

Email checklist

- **Before** emailing any external parties:
  - Check whether it is acceptable to send personal information.
  - Confirm the accuracy of the email addresses.
  - Check that everyone on the copy list has a genuine ‘need to know’.
  - Use the minimum identifiable information (e.g. NHS number).
  - Check encryption requirements.
- Where email needs to be sent to an unsecure recipient:
  - Check they understand and accept the risks or
  - If you can encrypt the email.

Phone breach

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

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

Phone checklist

- Where possible:
  - Confirm the enquirer’s name, job title and organisation.
  - Confirm the reason is appropriate.
  - Take a contact phone number, e.g. main switchboard 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 enquirer.
- Record your name and details about disclosure, along with the recipient’s details.

Fax breach

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

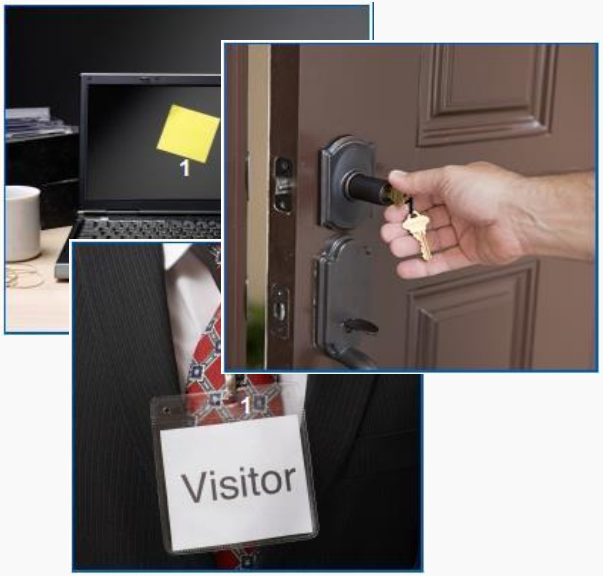
What happens - The fax goes to a local golf club where the manager calls the local newspaper. An embarrassing article about negligence and breach of confidentiality soon follows.

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

Fax checklist

- If it is absolutely necessary to send information by fax, if possible:
  - Fax personal details separately from clinical details.
  - Phone the fax recipient to inform them you are going to send confidential information.
  - Ask the recipient to acknowledge the fax.
  - Double check the fax number and use pre-programmed numbers.
  - Use a fax cover sheet.
  - Request confirmation that the fax was received.
  - Remove the original document from the fax machine.

Data security risks 1



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

Data security risks 2

- **Doors**: Nearly every door was open; even “restricted access” doors had been propped open to allow for a delivery.
- **Visitors**: The receptionist was happy to direct him to the server room…he wasn’t even asked to sign in or show a visitor’s badge.
- **Desks**: There was so much information in unoccupied office areas. He randomly dispersed memory sticks on the desks; hopefully someone will plug one into their machine and it can start installing malware.
- **Other areas**: The server room door was unlocked, meaning he could disrupt the server causing connectivity problems.
- As there is so little physical security, he can potentially come and go as he pleases…perhaps next week.

Summary

- In this presentation, you've heard why data security is important, the legal obligations for staff working in health and care, threats to the security of information, and how to identify a potential incident or breach.
- Hopefully you can now see why good data security is important, and why we are all bound by legal requirements to protect health and care information.
- You should complete the assessment to finish your training.

Module summary

- Having completed this session, you should understand:
  - The principles and terminology of information governance (IG).
  - Basic data security / cyber security terminology.
  - The importance of data security to patient/service user care.
  - That law and national guidance requires personal information to be protected.
- And be able to:
  - Explain your responsibilities when using personal information.
  - Identify some of the most common data security risks and their impact.
  - Identify near misses and incidents and know what to report.
  - Distinguish between good and poor practice when using personal information.
  - Apply good practice in the workplace.

Resources

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

References

1. Information Commissioner's Office. Chelsea and Westminster Hospital NHS Foundation Trust *monetary penalty notice*.
2. Department of Health. Confidentiality: NHS Code of Practice. London: DH, 2003.
3. The National Cyber Security Centre - Creating passwords: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0.
4. The National Cyber Security Centre - Password Managers: https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers