An Introduction to

Information Governance

Including

Health Records

Required to retain the confidentiality "declaration" prior to logging onto the IG mandatory module

Based on & Using the Health & Social Care Information Centre
Introduction to Information
Governance e-learning training tool.
Introduction to Data Security
Awareness
Refreshed for General Data
Protection Regulations

Contents

This course is split into 8 sections and includes an end of course assessment to complete. You must read through all the sections and then achieve a score of 80% in the assessment in order to meet your mandatory training requirement. The sections are;

Introduction

Confidentiality

Data Protection

Information Security

Freedom of Information Act 2000

Record Keeping

Health Records Management

Summary

Use the right arrow button on the navigation bar below to progress onto the next slide.

This can be used on all slides apart from question slides where the question must be attempted before being able to move on.

Introduction

In December 2007 it was widely reported in the national press that nine NHS trusts had misplaced thousands of patient and staff records.

Unfortunately since this time we have continued to read or hear about data losses in the media.

Our service users (patients) are much more sensitive and aware of their rights and what makes good Information Governance (IG) practice.

In this module you will look at the principles and procedures, in short ‘the rules’ that can help you to manage information safely and effectively.

Introduction/Information Governance (IG) and You

Processing information is any activity we perform with data (either paper or electronic) e.g. copying, adding, storing, filing and destruction. IG is to do with the rules that must be followed when we process information. It allows the Trust and staff within to ensure information is processed legally, securely, efficiently and effectively. IG applies to all the types of information which the Trust processes, but the rules may differ according to the type of information concerned.

This programme support you to:

- Understand the principles of Information Governance and how they apply in every day working environments
- Understand within the context of their specific role how to provide a confidential service to patients and service users in line with the duty of confidentiality
- Know how to ensure and maintain good record keeping
- Understand fundamentals of data protection, confidentiality and the Caldicott Principles
- Understand the responsibilities of healthcare organisations under the Freedom of Information Act 2000
- Understand individual responsibilities in responding to a Freedom of Information request
- Understand the principles of good record keeping
- Understand, within the context of their role, how they can apply and maintain information security guidelines
- Know where they can gain local access to policies, procedures and further information on Information Governance.

Introduction/**Data Types**

In health and care settings, you might see:

- Confidential information.
- Personal information.
- Sensitive Information “Special Category information”
- Anonymised information
- Pseudonymised information
- Corporate Information

These different types of information are defined further.

Introduction/Confidential and Personal Information

Personal data includes medical records and personnel records.

Information about individuals is personal information when it enables an individual to be identified. For example, a person's name and address are clearly personal information when listed together however an unusual surname may itself enable someone to be identified.

Personal information may be held subject to obligations of confidentiality and may be legally sensitive as defined by the General Data Protection Regulations/Data Protection Act 2018

Personal information is classed as **confidential** if it was provided in circumstances where an individual could reasonably expect that it would be held in confidence, e.g. the doctor/patient relationship. Confidentiality is generally accepted to extend after death.

Introduction/Sensitive "Special Category" Information

Personal information falling under the Special Categories of data is classed as **legally sensitive** when it makes reference to particular matters, such as **health**, ethnicity or sexual life that are listed in the General Data Protection Regulations/Data Protection Act 2018

Other details, for example an individual's bank account details would also be regarded as sensitive by most people but are not legally sensitive.

Introduction/Person-Based Anonymous Data

For example public health statistical information that does not identify an individual.

Person-based anonymised information does not identify an individual directly and cannot be reasonably used to determine identity.

It is important to be aware that person-based but anonymised information is not subject to the same restrictions on processing as personal information. This is because no-one can be harmed or reasonably distressed by its disclosure. Neither confidentiality law nor the Data Protection principles apply to person-based information that has been effectively anonymised.

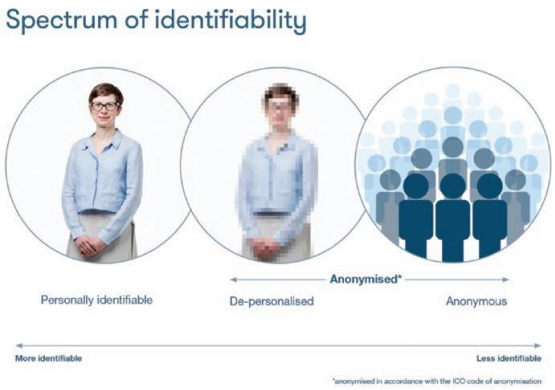
This means that taking steps to anonymise information is often very important as it enables information to be processed without having to satisfy strict legal requirements. Where you have a working requirement to use or convert cohorts of data into Anonymous formats, advice and support can be sought from the Informatics department.

Introduction/Person-Based Pseudonymised Data

This is information that does not identify an individual, because identifiers have been removed or encrypted. However, it would, in theory, be possible to reverse that process and re-identify someone, so safeguards are still important. Information processed in this format is captured by the Data Protection principles and needs to be treated with the same safeguards in place as identifiable information.

It is just like a blurred photo of someone, we can't immediately see how the person is, but we know it is a specific person. If we had the computer power, and really need to know who the person was, it might be possible to work it out. There are strict safeguards on how de-personalised/pseuduonymised information can be used and processed because there is the potential that it might be possible to re-identity someone.

If you have a working requirement to handle data in a pseudonymised way advice can be sought from the informatics team



Introduction/**Corporate Data**

Corporate Data includes information relating to the Trust, for example Trust accounts or statistical reports.

Documents or information that are not about individuals are clearly not personal information but may be classed as commercially confidential e.g. for commercial reasons or because they contain legal advice. They may also be regarded as sensitive in a general sense because of the subject matter.

An important consideration in relation to documents is whether or not they have to be disclosed when a Freedom of Information Act request is made and where they are confidential or sensitive they may be exempt from disclosure.

The Freedom of Information office can provide further support when required FOIRequest@SRFT.nhs.uk

Introduction/**Standards**

Standards are based on the following legislation:

The Confidentiality NHS Code of Practice and the NHS Care Record Guarantee for England

This Code tells you how to comply with the common law duty of confidentiality. The Guarantee tells patients how the NHS will use and protect the information in their health records.

The General Data Protection Regulations (2018) / Data Protection Act 2018

This European and UK legislation set rules for how personal data is obtained, held, used or disclosed.

The Freedom of Information Act 2000

This Act sets rules for disclosure of information about the work carried out by a public sector organisation.

The 2017/18 Data Security and Protection Requirements

This sets out the steps health and care organisations are expected to take to demonstrate that they are implementing the **ten data security standards**, recommended by Dame Fiona Caldicott, the National Data Guardian for Health and Care and confirmed by the UK Government in July 2017.

The Health and Social Care Act 2008

Places emphasis on the Trust to be open and transparent when using sensitive “Special Category” information, including those times when things go wrong (A Duty of Candour).

Introduction/**Standards**

Standards are based on the following legislation:

The Records Management NHS Code of Practice

This Code includes guidelines about how records, including health records, should be used and disposed of. This document holds the national retention periods.

The Information Security NHS Code of Practice

This Code sets out, at a high level, how organisations should comply with information security principles.

The Common Law Duty of Confidence

This is acknowledgement that past court cases, build foundations for future court rulings. In relation to the Trust, the Common Law Duty of Confidence extends the expectation of a patient to maintain the confidentiality of information given in a patient clinician environment to cover all staff at the Trust that may come into contact with that information for whatever reason. (eg filing clerk, MDT meetings, secretary)

Introduction/Scenario

Introduction/Your Responsibilities

IG provides the principles that supports staff carry out their responsibilities and comply with the law and best practice when processing sensitive "special Categories" information on a daily basis. Information Governance is everyone's responsibility and your key responsibilities can be summed up as:

- **Providing a confidential service to patients, sharing information lawfully and appropriately**
- **Processing information in accordance with the 'data protection rules' and respecting the rights of individuals**
- **Recording information accurately and ensuring it is accessible when needed**
- **Ensuring that information is held and processed securely**
- **Maintaing Records Governance standards (with paper and electronic) records**
- **Complying with Freedom of Information requirements**

Information Governance sets common guidelines that help NHS staff know they are working to the same standards as people outside their own area.

Introduction/**Scenario**

A famous footballer is rushed into surgery for an operation on a broken foot.

Several hospital staff spot the celebrity and some of them look up the player on the Electronic Patient Record, which includes a prior history of depression.

That evening, on the phone to a friend, one of the staff mentions the surgery and other health issues the footballer has.

The next morning, the story of the star's depression and surgery appears on social media and is splashed all over the front covers of the tabloids.

With pressure from the celebrity's lawyer threatening to sue the hospital unless all the culprits are found and disciplined, things are looking very bleak.

Introduction/**Scenario**

The Hospital carries out an internal investigation to identify the staff member(s) that viewed and those who then disclosed the information. If they were not directly involved with the patient's care, which of the following actions were the staff members not justified in doing?

a) Viewing the patient's healthcare record?

b) Sharing information relating to the patient's upcoming surgery?

c) Disclosing information relating to the patient's past healthcare history?

Introduction/Scenario Answers

None of the actions could be justified.

The breaches will lead to a disciplinary sanction in accordance with the Trust's disciplinary procedure or even dismissal. If the culprit that disclosed the information outside of the Trust turns out to be a clinician they could also be reported to their regulatory body, which may result in a professional misconduct committee to decide whether the breach of confidentiality warrants suspension or removal from the professional register.

This scenario would raise a number of dilemmas for the Trust. The duty to maintain confidentiality is part of the duty of care to the patient. It is also integral to the contract of employment and the individual's regulatory professional code of conduct. Additionally, compliance with the Caldicott Principles requires that patient information is only used on a 'need to know' basis. None of the staff needed to view the information to carry out their roles. Later you will see how the Caldicott Principles are applied to disclosure of sensitive personal information. The Duty of Candour placed on the Trust outlines the requirement to inform the patient when such incidents arise. The GDPR legislation sets out a requirement to notify the regulatory bodies within 72 hours of a breach occurring.

Confidentiality

To help prevent the kind of breaches in confidentiality seen in the previous scenario, there are certain procedures to follow.

Duty of confidence

A duty of confidence arises when sensitive “special categories” information is obtained and/or recorded in circumstances where it is reasonable for the subject of the information to expect that the information will be held in confidence. Patients provide sensitive “special categories” information relating to their health and other matters as part of their seeking treatment and they have a right to expect that we will respect their privacy and act appropriately. The duty can equally arise with some staff records, e.g. occupational health, financial matters, etc. Patients and staff have a right to be informed about how we will use their information for healthcare, the choices they have about restricting the use of their information and whether exercising this choice will impact on the services offered to them.

The Trust does this through privacy notices available on the website/intranet

Confidentiality

Legal requirement

Always remember confidentiality is a legal requirement, supported by the confidentiality clause in your contract and, where applicable, your professional code of conduct. The Trust is required to:

Ministry of JUSTICE

- Inform patients about how personal information relating to them will be used
- Inform patients of their right to object to the disclosure of their confidential personal information outside of the organisation
- Seek explicit and informed consent before disclosing patient personal information for non-healthcare purposes (unless a legal gateway exception applies).

Confidentiality/Sensitive "Special Categories" Information

Sensitive information is a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community. Certain types of information are classed as sensitive "special categories" under the Data Protection principles, but the definition for NHS Information Governance purposes is wider than, and fully encompasses, legally sensitive information.

It should also be noted that whilst the Data Protection principles apply to personal information relating to living individuals, NHS Information Governance also encompasses information about deceased individuals. During our working practices we are all bound to treat information of the deceased in the same regard to that of the living.

Legal Justification

Article 6, section 1(c) of the General Data Protection Regulations provides a lawful basis for processing where "processing is necessary for compliance with a legal obligation to which the controller is subject" As the Trust processes data classified as "special category" under the legislation we also need to meet a condition under Article 9, to ensure processing can be legally justified. Section 2 (h) sets out the condition for processing under "medical diagnosis the provision of health or social care or treatment or the management of health or social care systems". Staff should generally be aware that it is these conditions from Article 6 and Article 9 which permit the processing of patient/staff data and not the condition of consent.

Confidentiality/Sensitive "Special Categories" Information

Informing people

You should inform patient and service users that you are accessing and using their information

Explain	Give Choice
Clearly explain to individuals how you will use their personal information. Additional information about this is available in the Trust Privacy Notice	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 individuals 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/Sensitive "Special Categories" Information

Sharing information for care

Sharing information with the right people in a timely manner can be just as important consideration as one not to disclose information. Information Governance supports sharing, if in doubt you should seek assistance to document the correct purpose for the intended/requested data sharing; to map the most appropriate way to do this.

Note the duty to share for care where the right conditions are met.

Check – No surprises

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

Safe Best practices

Ensure that the data protection, record keeping and security best practices standards are met to support the sharing

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. For routine bulk sharing informatics reporting will take account of patients preference.

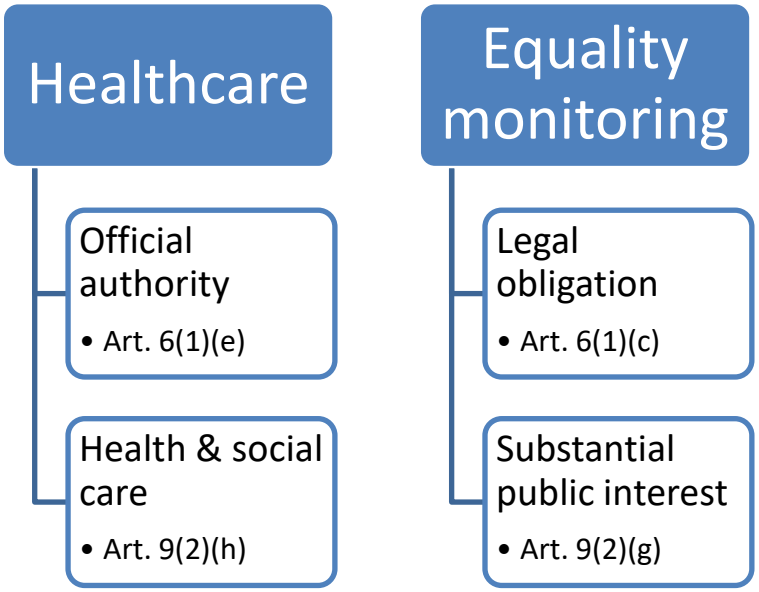
Confidentiality/Sensitive "Special Categories" Information

Sharing information for care

Across the Greater Manchester footprint there is a move towards Integrated Models of Care. The Information Commissioners data sharing code of practice specifies that "under the right circumstances, and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service …. but…. rights under the Data Protection must be respected. Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness."

There are many occasion in supporting our patients that we need to rely on the conditions of data protection to support sharing information in the right way to enhance the care we provide.

Your project lead, or information Governance lead can support you establish new processes and ways of working which support this sharing framework.



Confidentiality/The Caldicott Guardian

To help maintain levels of confidentiality throughout the NHS, a report was commissioned in 1997 by the Chief Medical Officer.

One of the key outcomes of this report was that Caldicott Guardians were appointed in each NHS Trust, in order to safeguard access to patient-identifiable information.

The Caldicott Guardian is normally at Board or Senior Management level as they are responsible for reviewing, overseeing and agreeing policies governing the protection of patient or personal information.

The Caldicott Guardian also takes responsibility for overseeing organisational compliance with the Caldicott Management Principles.

The Caldicott Guardian for the Trust (Salford) is Dr Peter Turkington, Medical Director.
The Caldicott Guardian for the Trust (Pennine) is Dr Roger Prudham, Deputy Medical Director

Confidentiality/The Caldicott Principles

A key recommendation of the Caldicott report was that staff justify every use of confidential information and routinely test it against seven principles. You must never disclose confidential information if you are unsure about your response to any of these six questions.

1. Do you have a justified purpose for using this confidential information?

The purpose for using confidential information should be justified, which means making sure there is a valid working reason for using it to carry out that particular purpose.

2. Are you using it because it is absolutely necessary to do so?

The use of confidential information must be absolutely necessary to carry out the stated purpose. Ask yourself if the information supplied needs to be person identifiable data? Always make the information anonymous where possible.

3. Are you using the minimum information required?

If it is necessary to use confidential information, it should include only the minimum that's needed to carry out the purpose in hand. Do you really need to supply their full name, date of birth (DOB) and full address? (A partial postcode will identify a geographical area if this is all that is needed)

Confidentiality/The Caldicott Principles

4. Are you allowing access to this information on a strict need-to-know basis only?

Before confidential information is accessed, a quick assessment should be made to determine whether it is actually needed for the stated purpose. Always Keep information Secure - Use passwords / locked filing cabinets / locked trolleys etc.

If the intention is to share the information, it should only be shared with those who need it to carry out their role.

5. Do you understand your responsibility and duty to the subject with regards to keeping their information secure and confidential?

Everyone should understand their responsibility for protecting information, all staff and those working on behalf of the Trust are accountable for protecting information they come into contact with. All staff must as a minimum complete Information Governance and Health Records Governance mandatory Training on an annual basis.

If the intention is to share the information, those people must also be made aware of their own responsibility for protecting information and they must be informed of the restrictions on further sharing (this is generally set out within a Data Processing Contract).

Confidentiality/NHS Code of Practice

6. Do you understand the law and are you complying with the law on Data Protection and Security before handling the confidential information?

There are a range of legal obligations to consider when using confidential information. Every use of patient-identifiable information must be lawful. The key points of legislation that must be complied with are the common law duty of confidentiality and under the General Data Protection Regulations and supporting Data Protection Act 2018

If you have a query around the disclosure of medical or other confidential personal information you should go to your Line Manager initially then the IG Manager if you are still not sure. For serious and complex issues your Manager should contact the Caldicott Guardian for advice and guidance.

7. The duty to share information can be as important as the duty to protect patient Confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients and service users within the framework set out by these principles.

Confidentiality/**NHS Code of Practice**

As well as the Caldicott Guidelines, you can also refer to the Confidentiality NHS Code of Practice model known as **'Protect, Inform, Provide Choice and Improve'** to help maintain a confidential service within the Trust.

- You should protect a person's information by recording relevant data accurately, consistently and keeping it secure and confidential.
- Write patient records appropriately – free of jargon or offensive, subjective or opinionated statements.
- Inform a patient how their information is used and when it may be disclosed.
- Where practical, provide patients with the Trust's leaflets regarding confidentiality or point them to a copy of this on the Trust website. Also, inform patients of their right to access their health records.
- Provide choice for patients to decide whether their information can be disclosed. Patients have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them (in instances where the Trust has no legal gateway to make the release)
- As long as the patient is competent to make such a choice and where the consequences of the choice have been fully explained, their decision should be respected.

Continued

Confidentiality/NHS Code of Practice

- Always look to improve the way you protect, inform and provide choice to the patient, clients and employees. You can do this by seeking line manager support and by reporting possible breaches via DATIX.
- You can find out more about this model within the Confidentiality NHS Code of Practice. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

- **Personal Information also relates to staff.**
  - **Remember you are breaking the law if you access the health records of another individual without a working right to do so. Disciplinary action will be taken against any staff who are found to do this and this may result in dismissal.**

Confidentiality/**Summary**

You've now completed the topic on confidentiality.

Confidentiality is key to Information Governance, and the models you've looked at should help you improve your awareness. In particular, you can refer to:

- The Caldicott Guardian
- The seven Caldicott management principles
- The 'Protect, Inform, Provide Choice and Improve' model for providing a confidential service to patients.

Data Protection

Data protection issues can crop up in any organisation. The Trust takes the responsibilities of the legislation to its heart and outlines to all staff that we are each accountable for compliance with the principles.

Data Protection Act 2018

Breaches can occur because staff are unaware of data protection principles (contained in the General Data Protection Regulations and supporting Data Protection Act 2018) and how these are applied in their everyday processes. Couple of the most common errors include

- For getting to lock the PC screen when staff need to leave a PC suddenly
- Sharing data wider than intended – say via email
- Lack of checks with patient demographics – to ensure the correspondence is going to the right person
    - address on a letter goes to the wrong house
    - discharge summary printed and given to wrong patient

In this topic you are going to look at a series of data protection issues that may occur in the everyday running of the Trust. These are intended to support you in your everyday activities, however remember additional support can always be sought from the Caldicott Guardian, Data Protection Officer, SIRO (Senior Information Risk Officer) and Information Governance staff.

Data Protection/**The Law**

The General Data Protection Regulations and supporting Data Protection Act 2018 apply to all organisations in the UK that process personal information.

The Regulations go hand-in-hand with the common law duty of confidence and professional and local confidentiality codes of practice to provide individuals with a statutory route to monitor the use of their personal information.

A breach of one of the Data Protection Principles can result in legal action being taken against an individual and/or the Trust. Learning and applying the Data Protection Principles is therefore very important. Setting the principles within our day to day processes to maintain compliance.

There are additional offences around unlawfully obtaining, disclosing or selling personal data.

Links to the Computer Misuse Act 1990 and the Principles of Data Protection around security, provide additional legislations against sharing passwords, and entering information when logged onto a system using a colleagues account. Disciplinary action will be taken against any staff who is found to do this and this may result in dismissal and/or criminal proceedings.

Data Protection/**Principles**

1. Processed lawfully, fairly and transparent

Ensure that the proposed use of the information is lawful in the widest sense, e.g. doesn't breach other legal restrictions such as the common law duty of confidentiality.

Inform patients why you are collecting their information, what you are going to do with it, and who you may share it with.

Information recorded as part of the process of providing care should not be used for purposes that are unrelated to that care.

When formulating a research project remember to be open and transparent about what you will be doing with the information.

There should be no surprises! Be open, honest and clear.

2. Processed for a specified , explicit and legitimate purposes

Only use personal information for the purpose for which it was obtained. eg personal information on a Patient Administration System must only be used for healthcare purposes - not for looking up friends' addresses or birthdays.

Only share information outside the Trust, team, ward, department, or service if you are certain it is appropriate and necessary to do so.

If in doubt, check first!

Data Protection/**Principles**

3. Adequate, relevant and not excessive

Only collect and keep the information you need.

Do not collect information “just in case it might be useful one day!" You cannot hold information unless you know how it will be used and it is a justified use.

Explain all abbreviations, use clear legible writing and stick to the facts – avoiding personal comments and opinions, stick to clear language and avoid jargon .

Only what we need

4. Accurate and kept up-to-date

Take care when entering data to make sure it is correct.

Make sure you check with patients that the information is accurate and up-to-date at each contact with the patient

Check existing records thoroughly before creating new records and avoid creating duplicate records. Be continuous of data which is repeated in several systems.

Check personal details at each attendance

Data Protection/**Principles**

5. Not kept in a from which permits identification of individuals for longer than is necessary

Follow retention guidelines set out by the Records Management NHS Code of Practice and the Trust's retention of personal information.

Make sure your information (electronic and paper) gets a regular "spring clean" so that it is not kept "just in case it might be useful one day!"
Dispose of information correctly, according to the Trusts disposal policies

Place copies of paper records in the confidential waste at the end of the day. (hand over sheets)

6. Processed in accordance with rights of data subject

Individuals, whether staff or patients, have several rights under the legislation

- The right to be informed
- The right of access to personal data held about them (Subject access requests)
- The right to rectification
- The right to erasure
- The right to prevent processing likely to cause damage or distress
- The right to data portability
- The right to object
- Rights in relation to automated decision-taking, including profiling

The rights are not absolute, that means there may be occasions where the Trust is permitted to override them.

Data Protection/**Principles**

7. Protected by appropriate security

This requires that all organisations that process personal information have security measures in place to ensure that the information is protected from accidental or deliberate loss, damage or destruction.

The Trust has a number of security policies and processes to ensure the security of personal information. The Trust also has guidelines for staff about how to ensure personal information is protected from unauthorised access.

You must make sure you comply with all the security processes and guidelines so that access to personal information is only available to those authorised to do so, and information is not accidentally or deliberately lost, damaged or destroyed.

Some of the measures you should comply with are:

- Ensure confidential conversations cannot be overheard
- Keep your passwords secret and never log onto a system using a colleague's account
- Lock paper files away when they are not in use, Lock screens when you have need to leave the PC, maintain a clear desk at all times.
- Take due care and attention when printing document for patients only give to a patient information which relates to them, check the bundle you have picked from the printer – was it all intended for this purpose.
- Ensure transfers of personal information is always by secure methods, ensure information being sent by email is going secure (post, fax, digital)
- Only access records to which you have a legitmate right to access.

Data Protection/**Principle 1: Processing Conditions**

As you have just seen, Principle 1 of the Data Protection Act requires that personal data is processed fairly and lawfully. It also requires that personal data is only processed if one of the conditions is also met.

Processing conditions

There are several of these "processing conditions", but the main ones that you need to be aware of when providing care and treatment are processing:

- for medical purposes
- where the patient has given their explicit informed consent
- To protect the vital interests of the patient or another person
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority

Processing for medical purposes

This means that sensitive "special Categories" personal data can be processed for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care, or treatment or the management of health and social care systems and services.

Data Protection/Principle 1: Processing Conditions

Consent

If you wish to process patient information for purposes other than healthcare, in most cases you must have the explicit consent of the patient to do so.

Definition of consent

Consent must be freely given, specific, informed and an unambiguous indication of the data subjects (staff and patients) wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Data Protection/Principle 6: Processed in accordance with the Rights of Individuals

These are the key rights under the legislation applicable to the Trust.

The right to be informed

All individuals (patients and staff) are entitled to be informed of the purposes to which the Trust intends to use their information. Each and all purposes must have a lawful basis. The Trust has a Privacy Notice, available on the website which outlines the various purposes to which we use individual's information.

Subject access requests

Generally, individuals (staff and/or patients) have the right to see information about them held and processed by the Trust. Applications, which are known as "subject access requests" can be verbal or in writing and the individual should provide the Trust with sufficient information to enable their records to be correctly identified. The request must be complied with within one month of receipt but wherever possible information should be provided within 21 days.

Therefore, if you receive a request for information, (this can be formal or informal request) you should promptly forward it to the Information Access Department. Types of requests you might receive which fall under this provision could be, copies of letters sent to a patient years ago, copies of old results.

Data Protection/Principle 6: Processed in accordance with the Rights of Individuals

The right rectification

An individual who believes that the Trust has recorded inaccurate personal information about them is entitled to have this corrected. This right applies to factually incorrect information only, not to opinions or a diagnosis that the patient disagrees with or which turns out to be wrong. Should you be approached by a patient in this regard, they should initially be referred to their clinician for local resolution or the complaints/information governance department if escalation is required for resolution. The right extends to the completion of incomplete data, including a right to add supplementary statements.

The right erasure

An individual is entitled to this right under one of the following conditions:-

- The Trust has retained data for longer than necessary
- When the individual withdraws their consent (only valid where the initial lawful basis for processing was consent)
- When presented with an objection with no overriding interest
- When the Trust processing of data is found to be unlawful
- On occasions where there is a legal obligation on the Trust to comply with the erasure
- In instances where data was provided to a website by the individual when they were a child

Data Protection/Principle 6: Processed in accordance with the Rights of Individuals

The right to restrict processing

This applies where an individual believes that the Trust has recorded inaccurate personal information about them is entitled to send a written notice to the Trust requesting that processing of their data stop, or does not begin. The individual must be able to show that he/she has suffered or would suffer substantial and unwarranted damage or distress if the processing goes ahead. The Trust doesn't have to comply where the Trust believes that the processing is so important it must go ahead even though it causes damage or distress. This right also applied to any unlawful processing identified by the Turst, where data is no longer legitimately required by the trust (retention), under conditional of legitimate interest dispute.

The right to data portability

This gives individuals the right to receive data in a structured, commonly used machine readable format where original processed through consent or contract and processing is automated. Also where possible gives individuals the right to have data directly transmitted to another data controller.

The right of portability applies where data is processed under the condition of consent or contract, in majority of cases, the Trust processes data under a legal obligation condition.

Data Protection/Principle 6: Processed in accordance with the Rights of Individuals

The right to object

This gives individuals the right to object to their data being processed in any form by the Trust, this includes profiling. Unless the Trust can demonstrate compelling legitimate grounds for the processing which override the interest of the individual, then the right is upheld.

Where the Trust undertakes any direct marketing activities, an individual has the right to object at any time to receiving related messages.

Rights in relation to automated decision making

The individual can ask for the Trust to ensure that no decision which is taken by or on behalf of the Trust and significantly affects the individual is based solely on information processed by automatic means.

Data Protection/Principle 6: Processed in accordance with the Rights of Individuals

(NB – this is new page would need different header – Data Protection/Data Protection impact assessments

Data Protection Impact Assessment – What are these.

A Data Protection Impact Assessment (DPIA) is a process to help staff within the Trust identify and minimise the data protection risks of a project. This can be a new project, or revision to an existing system or process.

The requirement to complete a DPIA has moved from good practice to mandatory under GPDR when processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing.

When do I need to do one?

As Medical data is classified as Special categories data under the Act, any system or process processing patient data is likely to fall under the high risk remit for these risk assessments.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Data Protection/Principle 6: Processed in accordance with the Rights of Individuals

What does a DPIA involve?

A Data Protection Impact Assessment must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The Trust has template Privacy Impact Assessments, which will help project leads to assess any risks to patients or the Trust from the project allowing time in the implementation stage to mitigate the risks allowing the project to go ahead. Only in extreme case of risk would a project be stopped

Data Protection/Principle 6: Processed in accordance with the Rights of Individuals

In completing a DPIA the project lead may need to call on support from the supplier/data processors, Information Asset Owner, Data Protection Officer, where appropriate other relevant experts.

In instances where high risk is identified that you cannot mitigate, the Trust is obliged to consult the ICO (Information commissioner office) before starting the processing.

Data Protection/**Scenarios**

In the following screens we will look at a range of everyday scenarios where the data protection act comes into play.

Data Protection/Scenario 1: Unexpected News

Hospital staff: *"... No, calm down Mr Jones. This is just to let you know that your wife Sally is in labour - her waters broke an hour ago."*

Mr Jones: *"Oh. She's my ex-wife,* ***actually.*** *She ran off with my ex-best mate 5 years ago. I'm definitely no longer her Next of Kin. The divorce was finalised a while ago."*

Which two of the following data protection principles are being breached in this scenario?

a) Principle 1: Processed lawfully fairly and in a transparent manner

b) Principle 2: Processed for a Specified, explicit and legitimate purpose

c) Principle 3: Adequate, relevant and not excessive

d) Principle 4: Accurate & kept up-to-date

e) Principle 5: Not kept for longer than necessary

f) Principle 7: Protected by appropriate security

Data Protection/Scenario 1: Unexpected News

Hospital staff: *"... No, calm down Mr Jones. This is just to let you know that your wife Sally is in labour - her waters broke an hour ago."*

Mr Jones: *"Oh. She's my ex-wife,* ***actually.*** *She ran off with my ex-best mate 5 years ago. I'm definitely no longer her Next of Kin. The divorce was finalised a while ago."*

The following Principles have been breached;
Principle 1: Processed lawfully fairly and in a transparent manner
Principle 4: Accurate & kept up-to-date

By informing Mr Jones of his ex-wife's condition, the receptionist unlawfully breached Mrs Jones' confidentiality.
Also, the records being used here were obviously very out-of-date. If the patient had been asked whether her contact details were still correct when she came in for previous appointments, this mistake wouldn't have happened.

Data Protection/Scenario 2: Subject access request

Mrs Foster has sent an email asking her specialist for a copy of all her historic results from her health records held by the Trust. The secretary prints the email and passes it to the Data Protection Lead who puts it on top of his to-do pile. Later the pile is accidentally knocked over and the letter slips behind the desk

After two months Mrs Foster contacts the hospital to ask what is happening with her request. She is put through to the Data Protection Lead's extension, and hears a voicemail that the Lead is on holiday. The call is put back through to switchboard and Mrs Foster enquires whether there is anyone else that can help her. Unfortunately, the switchboard operator has never heard of IG so is unaware that there is anyone else she can refer Mrs Foster to.

She puts the call through to Trust Headquarters and one of the staff there takes Mrs Foster's details and promise to get back to her. No-one does. Seven days pass and Mrs Foster has still not been contacted, so she decides to ring the Information Commissioner to complain.

Data Protection/Scenario 2: Subject access request

Which of the following data protection principles are being breached in this scenario?

a) Principle 1: Processed lawfully, fairly and in a transparent manner

b) Principle 3: Adequate, relevant and not excessive

c) Principle 4: Accurate & kept up-to-date

d) Principle 6: Processed in accordance with rights of data subject

e) Principle 7: Protected by appropriate security

Data Protection/Scenario 2: Subject access request

The following Principles have been breached;
Principle 6: Processed in accordance with rights of data subject

Principle 6 (*Processed in accordance with rights of data subject*) requires compliance with the individuals rights set out in article 14 (section 3) of the legislation

One of these rights is the right to subject access, which means that individuals have the right, with some limited exceptions, to see information held by organisations that are processing their personal data.

Organisations are required to comply with the request within set time limits. You looked at some of the individual rights earlier in this topic.

Data Protection/Scenario 3: An Administrative Error

Sharon, an MDT co-ordinator collates all the papers necessary for a review meeting.
She decides that there is not enough space in her office to collate of the papers for the complexes cases this week, so she finds a quiet meeting room in the Post Grad Centre to do it instead.

She pops out to a M&S for lunch, leaving the notes unattended and the room unlocked.

Which of the following data protection principles are being breached in this scenario?

a) Principle 1: Processed lawfully, fairly and in a transparent manner

b) Principle 2: Processed for a specified explicit and legitimate purpose

c) Principle 3: Adequate, relevant and not excessive

d) Principle 4: Accurate & kept up-to-date

e) Principle 5: Not kept for longer than necessary

f) Principle 7: Protected by appropriate security

Feedback

The following Principles have been breached;
Principle 7: Protected by appropriate security

Sharon has breached Principle 7 of the legislation by not ensuring that access to the health records was protected, either by locking the door or taking the records back to the correct storage area.

Staff are to be aware the same principle applies here, where data accessed on a computer is not secured when leaving the PC, by locking the screen.

Data Protection/Scenario 4: Establishing a text reminder service

The Trust is considering setting up a text reminder service for outpatient appointments through a 3rd party company. The Outpatient team want to record mobile numbers for all patients to support issuing a text reminder in an attempt to reduce DNA rates

Which of the eight data protection principles would need risk consideration to ensure no breach of information occurs from this initiative?

a) Principle 1: Processed lawfully, fairly and in a transparent manner

b) Principle 2: Processed for a specified, explicit and legitimate purpose
c) Principle 3: Adequate, relevant and not excessive

c) Principle 4: Accurate & kept up-to-date

d) Principle 5: Not kept for longer than necessary

e) Principle 7: Protected by appropriate security

.

Data Protection/Scenario 4: Establishing a text reminder service

Feedback

The following Principles need key consideration before the project goes ahead;

Principle 1: Processed lawfully, fairly and in a transparent manner
Principle 2: Processed for a specified, explicit and legitimate purpose
Principle 3: Adequate, relevant and not excessive
Principle 4: Accurate & kept up-to-date
Principle 5: Not kept for longer than necessary
Principle 7: Protected by appropriate security

Principle 1 requires that personal data is processed fairly; in this instance the Trust intends to release data to a 3rd party without having identified the legal justification for do so. Under Principle 1 a Privacy Impact Assessment should be carried out which will highlight that individuals should be informed of the purposes for which their data will be processed and who it may be disclosed to. In this instance the justification will be continued health care.

The notification to patients is normally done by use of a privacy notice setting out the list of purposes and other information regarding who may have access to the information. Information about patient home addresses and contact details is generally provided for the support of patient care. The Trust must stipulate that text messages are to be for appointment reminders only and to be used for other purposes (such as recommending new drugs on behalf of a pharmaceutical company). Through the PIA,

Data Protection/Scenario 4: Establishing a text reminder service

the Trust will be able to document that this is part of the care pathway that the right conditions have been put in place with the suppliers and in fact no breaches of data protection will be made.

The PIA will also highlight that a Data Processing Contract needs to be in place with the 3rd party which stipulates the standards under which they must process the data to support the text message solution for the Trust.

Principle 2 requires that information provided for one or more specific purpose should not be used in a way incompatible with those purposes. Keeping text message related to medical appointments only will be in line with principle 2. Issuing text message to make a charitable donation to the Trust would not. Additionally, in supplying the list to the supplier the Trust must honour any notifications previously made by patients to opt out of receiving communications by text.

Principle 3 requires that data used for the project is not excessive. The Trust would need to put processing in place with the 3rd party to only release the mobile phone number and details of the message that needs to be sent. No names, address, dates of birth need to be sent to the supplier to support the release of text messages.

Data Protection/Scenario 4: Establishing a text reminder service

Principle 4 the project team leading the text message implementation will need to ensure that the Trust has processes in place to support the accurate data collection of mobile phone numbers for patients. Review the need to change recording mechanisms for mobile contact numbers on PAS or other systems. This need will come out of the Privacy Impact Assessment review.

Principle 5 – outlines that data must not be kept for longer than necessary. As part of the project it will be necessary for the Trust to stipulate with the supplier the timelines for destruction of data. Both during the contract period and in the event the contract is ended.

Principle 7 – outlines that the Trust needs to ensure the security of the data. As part of the Privacy Impact Assessment the project team will map the flows of data needed to support the text message service. The result will be assurances that when the data is held by the Trust within PAS, it is held secure. That in transfer to the 3rd party supplier data is encrypted. When data is with the supplier being processed checks have been made that they have appropriate security standards equivalent to that of the Trust to support the secure processing of the data needed to send the text messages.

Data Protection/Scenario 5: Retaining Records

Meg is a new ward clerk at the Trust. She has been asked to check the storage room and dispose of any old patient admission books. Each book comprises over 100 records containing a patient's name, address, hospital number, consultant, admission reason, and dates of admission and discharge.
The ward manager asks her to get rid of any books which are more than 10 years old. The store-room contains dozens of the books and Meg finds two that are over 12 years old. This exceeds the recommended maximum 8 year retention period in the Records Management NHS Code of Practice

Which of the eight data protection principles is being breached in this scenario?

a) Principle 1: Processed lawfully, fairly and in a transparent manner

b) Principle 4: Accurate & kept up-to-date

c) Principle 5: Not kept for longer than necessary

d) Principle 6: Processed in accordance with rights of data subject.

e) Principle 7: Protected by appropriate security

Data Protection/Scenario 5: Retaining Records

The following Principles have been breached;
Principle 5: Not kept for longer than necessary

To comply with Principle 5 the Trust should regularly review the personal data held in line with record retention standards and delete information that is no longer required for the purposes for which it was obtained. In this case, the personal data was obtained for the purpose of recording a patient admission to a particular ward over 12 years ago. The information was retained to provide a record of which patients were also on the ward at the same time. However, it is unlikely that this information is still required and it should have been disposed of some time ago.

Disposal does not necessarily mean destruction and care should always be taken to do things right when destruction is required. More information on record retention and disposal is provided in the Records Management NHS Code of Practice.

Data Protection/Scenario 6: Information for sale

James is an administrations clerk at the Trust, currently involved in patient registrations. One morning on his way to work he is approached by a man claiming to be a private detective hired to locate the beneficiary of a will.

The detective explains to James that he believes the woman is living in the area and could possibly be a patient of the Trust. He asks James to look through the registration records and supply the woman's address if she is registered.

James knows he shouldn't really do this, but the detective assures him that the woman will be pleased that he has helped. He also offers James £100 if he provides the information before the end of the working day.

James locates the details in Patient Centre, but speaks to a colleague before handing them over. He tells James that he has broken rules just by accessing the details and advises him to inform the IG team and the hospital security team about the detective.

Data Protection/Scenario 6: Information for sale

Would James have breached the Data Protection Act by providing this information?

a) No, the woman would want to know that she had been left something in the will.

b) It depends whether he accepts the £100.

c) No, James would have only provided the woman's address, this isn't personal data.

d) Yes, James would have unlawfully disclosed personal data.

Data Protection/Scenario 6: Information for sale

Yes, James would have unlawfully disclosed personal data and therefore breached the General Data Protection Regulation.

The address is personal data because it relates to a living individual who can be identified either solely with that data or with other information already available. The detective already has the woman's name and if James had supplied the address this would enable accurate identification.

The disclosure would be a criminal offence under the legislation. James had not been given authority by the Trust to supply this information It makes no difference whether or not he accepts any money for the information. James could have easily referred the matter to his IG Lead, who if necessary can contact the woman and ask whether she wants this information given to the detective

Data Protection/Scenario 6: Information for sale

Is it permissible to:

View your own health records?

Check which ward a colleague has been admitted to, to pop up with good wishes and a card?

Check an appointment time for a relative?

Check a result for a blood test you have had taken?

Get somebody's address from PAS/Patient Centre to send them a birthday card?

Check how a patient is that you looked after a year ago?

NO!

You can only access records you have a working requirement to view.
You cannot access any of your personal records without raising a subject access request.
No one has immediate right of access to a health record.

Data Protection/**Summary**

You should now have a good idea of what the legislation requires from you in terms of personal data processing.

By working through the scenarios in this topic, you have looked at how the General Data Protection Regulations and supporting Data Protection Act apply in practice.

The Freedom of Information (FOI) Act 2000

If you received a letter from a patient requesting a detailed breakdown of your organisation's expenditure for the year, would you know what to do?

The Freedom of Information Act 2000 requires disclosure of information by public authorities, such as NHS Trusts, County Councils and Government departments.

To support centralised processing of such requests the Trust has a Freedom of Information team.
Any requests received should be forwarded to FOIRequest@SRFT.nhs.uk

Freedom of Information Act 2000

FOI Act 2000/**Exemptions**

There are several exemptions within the Act, giving circumstances where the Trust does not have to provide the requested information.

The exemptions you may need to know about are where:

- The applicant could easily obtain the requested information from elsewhere
- The organisation already has published or has firm plans to publish the information

(The Trust has a proactive approach to release of information in the spirit of opens and transparency, each service should regularly review information it posts to the website and consider its accuracy and if any additional information the public may be interest to see should be posted)

- Or where the information:
  - Relates to confidential business information
  - Is personal information about the applicant
  - Is personal information about someone other than the applicant and disclosure of it would breach Principles of the Data Protection legislation e.g. it is confidential to a third party.

Unless an exemption applies, information must be supplied if a request is received.

It should also be noted, that were data is not held (i.e. where we are asked for an opinion) there is no obligation to create data in order to respond to an FOI request.

FOI Act 2000/What you need to know about FOI

Which is a Freedom of Information Request?

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

FOI Act 2000/What you need to know about FOI

Feedback

Example A is a subject access request and should be dealt with under the Data Protection legislation.

Example B is not asking for personal information and is asking for information about the practice (NB – under the FOI legislation GP practices are classified as a public body) which an exemption could not be applied to.

Example C is a request for personal information on behalf of a third party and would be processed by the Health Records Department.

Example D is not asking for personal information and is asking for information about the Trust which falls under the FOI Act to release to which an exemption could not be applied to.

Example E is not asking for personal information and is asking for information about the Trust which falls under the FOI Act to release to which an exemption could not be applied to.

Example E is not asking for personal information and is asking for information about the Trust's plans for spending and utilisation of public funds which falls under scope of the FOI Act. Consideration would be given to release papers on proposed closures, where there are no documented plans the Trust is under no obligation from the Act to create plans in response to the request.

FOI Act 2000/What you need to know about FOI

Types of information

The FOI Act gives the public the right to request any information held by any type of public authority or by persons/organisations providing services for them.

This includes educational institutions, NHS Trusts and contractors, Local Authorities etc.

The public can request information held within things like minutes of meetings, work emails, work diaries, corporate reports and other work documents. Exemptions may apply for certain information, which therefore would not be disclosed.

Form of request

Requests for information must be made in writing but there is no need for the applicant to mention the FOI Act. (In writing can include by email, Twitter, facebook or letter)

If a patient or member of the public asks you for information that you think is covered by the FOI Act, you should ask them to put their request in writing or assist them to do so. (for example details on the referral criteria for a service)

An applicant need not provide their true name in the request, but there must be a valid address for correspondence, which can be a postal address or an email.

Processing requests

If you receive a request for information, you should promptly forward it to the Freedom of Information Team (within Digital)

Response time

Generally, the organisation must comply with requests for information within 20 working days.

If the Trust decides not to provide the requested information the applicant must be informed of this and in most cases he/she must also be told why the information has been withheld.

FOI Act 2000/Breaches of the Act

A criminal offence is committed if requested information is altered, defaced, blocked, erased, destroyed or concealed with the intention of preventing disclosure of any or part of the information.

Liability

Both the Trust, i.e. the legal entity, and the employee that prevented disclosure of information are liable to conviction. The Information Commissioner can take action through the issuing of notices if a complaint is received about the way a request for information has been handled.

Information notices

The Information Commissioner can issue an information notice that requires the organisation to provide information relating to the particular request that has resulted in the complaint.

Enforcement notices

If the Information Commissioner believes that an organisation is not complying with the Act, she can ssue an enforcement notice requiring compliance within a set timescale. This might relate to providing information that has been incorrectly withheld.

FOI Act 2000/Breaches of the Act

Decision notices

Here the Information Commissioner can issue a decision notice stating that a request for information has or has not been properly handled. If the decision is that the organisation has not handled a request adequately, the Information Commissioner will set out the steps that need taking to ensure compliance.

Failure to comply

If the Trust fails to comply with any one of the notices issued, the Information Commissioner can refer the matter to the High Court who can deal with the matter as contempt of court.

FOI Act 2000/Case Study 1: A call to Action?

The Trust receives a phone call from an anonymous source requesting details about the Trust's annual income and expenditure report.

Caller: *"Hi, yeah. My name's Jeff and I want to know how much money the hospital makes and your general expenditure. I want exact amounts and would like you to get me the details by the end of the week."*

The receptionist advises him to put his request in writing to the hospital and informs him that a response will follow once the request is received.

Later that day, the patient advisory liaison service team (PALS team) receives an email requesting the information. They forward the email to the person responsible for dealing with FOI requests within the Trust, who decides there is no need to disclose the information as it is readily available elsewhere and they have firm plans to publish their annual report.

FOI Act 2000/Case Study 1: A call to Action?

A response is emailed to Jeff informing him that this information is within the Trust's annual report, which is published on the Trust's website. He is also informed that if he requires next year's report, they have plans to publish this at the end of the next financial year, usually by 6th April. A link to the trust website is also provided in the response.

Select the reason you think the FOI Lead had for not sending the information requested once the written request was received.

a) The applicant didn't give their name.

b) The applicant made the request by telephone.

c) Information was accessible elsewhere

d) The applicant didn't state that he was requesting the information in accordance with the FOI Act

e) The applicant wasn't very polite

FOI Act 2000/Case Study 1: A call to Action?

The FOI Lead did not send the information as it was accessible elsewhere.

As the information requested by the applicant could easily be obtained from the Trust's website, and there was an intention to publish the latest annual report in April, the Trust was not obliged to comply with the disclosure request.

It should be noted, the person requesting the information is not required to disclose their true identity and neither do they have to mention the Freedom of Information Act.

FOI Act 2000/Case Study 2: Art Attack

A children's ward has recently been redecorated as part of an integrated Care in the Community project. A patient's father is not happy with the equipment being used in the ward.

Mr Heath, the father of one the patients, writes a letter to the hospital stating, 'I find it outrageous that you have invested money in decorating the walls of the ward when it could be much better spent on medical equipment.

'I would like to know if the medical equipment in the children's ward has been PAT (Portable Appliance Testing) tested. Are procedures in place to ensure this happens regularly and are there any plans to buy equipment in the near future?'

The Trust Freedom of Information lead sends a letter responding to Mr Heath informing him of all policy and procedures in place for keeping portable medical equipment maintained to the required standard.

FOI Act 2000/Case Study 2: Art Attack

The Trust Freedom of Information lead sent the letter to Mr Heath within one week after receiving the written request. He includes the following in the letter:

- A link to these documents on the Trust publication scheme website
- A copy of the most recent PAT report for this particular ward
- A list of new equipment ordered and due to be delivered by March of this year.

Was this FOI request dealt with efficiently and according to the terms of the FOI Act?

a) Yes

b) No

FOI Act 2000/Case Study 2: Art Attack

Yes, this FOI request dealt with efficiently and according to the terms of the FOI Act.

Part of the information was available already so the applicant was directed to where this information could be located, in line with the exemption that the information is available elsewhere. The second part of the request was held by the Trust but not published. This information was disclosed as a valid request was received and the Trust responded correctly by sending a copy of the 'new equipment order list' and the PAT report. Additionally, the request was processed and responded to within the 20 working days as required by the FOI Act 2000.

FOI Act 2000/**Minimising Complaints**

Many of the complaints concerning FOI requests are about organisations not responding to applicants in a timely fashion.

Because of the tight timescales it is vital that if you receive a request for information you forward it to the Freedom of Information office (email account FOIRequest@SRFT.nhs.uk) as soon as possible.

It is also important that you comply with good record keeping principles, such as using logical file names for records and documents so that they can be easily located if requested.

You will explore good record keeping in a later topic.

FOI Act 2000/**Summary**

You have now reached the end of this topic on the Freedom of Information Act.

In this topic you have covered:

- The basic principles of the Freedom of Information Act
- The types of information that can be requested
- How a request should be made
- Some of the exemptions that permit withholding of information
- The short timescale for complying with a request
- The criminal offence of intentionally preventing disclosure of information
- The notices that can be issued by the Information Commissioner if an applicant complains about how you handle a request
- The penalty for not complying with a notice from the Information Commissioner.

Record Keeping

Bob comes to A&E with a chronic breathing condition. The receptionist completes an A&E attendance for him and finds out that he has attended A&E six times in the last two months.

The Nurse checks the Patient Administration System for Bob's case notes but doesn't seem to have any record of his previous visits.

The Consultant asks the medical records staff for Bob's paper case notes, but they cannot find them in the records library. They don't have any tracking system in place to know whether another consultant had requested the notes and not returned them.

The filing guidelines had been neglected by the medical records team as they have been too busy carrying out a housekeeping task to archive old records. Files have been left in huge piles but in date order to be filed later when they have time.

As a result Bob was admitted and a new set of paper records were created

Record Keeping

There are four record keeping risks highlighted in Bob's case.

1. Lack of history
The case notes from previous visits were not logged on the electronic system. This can be a risk to patients as the lack of history means the next team of clinical staff dealing with Bob's care would not have all the information they need. What if Bob was unconscious? How would they have known about the previous visits and missing case notes?

Tracking records, applied to records of all types held by the Trust, this can be corporate, health or staff records. It is important that records are registered and their location is understood. Records need to be located at the point of need, no matter the type of record they are.

Record Keeping

There are four record keeping risks highlighted in Bob's case.

2.Rrecords not tracked

Within medical records staff were not working according to Trust guidelines. Medical records are not being tracked when taken out and when returned to the records library.

Staff should note that all Supplementary/loose leaf notes are to be tracked

Record Keeping

There are four record keeping risks highlighted in Bob's case.

3. Case notes not filed in a timely manner
Case notes are left in heaps and not being filed in a timely manner, which means that if a patient visits the hospital again soon after the first visit, key information will be missing from their medical record, as in Bob's case.

It is important to make timely (contemporaneous) entries into medical records (in both paper and digital format)

Record Keeping

There are four record keeping risks highlighted in Bob's case.

4. A duplicate record has been created
The final action to create a new medical record for Bob is necessary in this case but represents very poor practice, as this means a duplicate record is created with only a partial medical history. This could be a risk to the patient and have a huge impact on the care delivered by the clinical team.

This topic will provide you with information about good record keeping and about what you can do to ensure records are complete, accurate, and available where and when needed.

Record Keeping/What is a Good Record?

a) Legible writing

b) Complete, i.e. all the information in one place

c) Including accurate information

d) Written contemporaneously, i.e. at the time an event occurred

e) Easy to locate

Feedback

All of these things are essential to good records keeping.

The Trust needs to make sure the information contained within its records are good quality.

Poor quality information is dangerous and presents a high risk to the organisation, the staff and the patients.

Record Keeping/What is a Good Record?

Senario

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

Record Keeping/Recording Quality Information

Commitment 8 of the NHS Care Record Guarantee promises patients that the NHS will take appropriate steps to make sure personal information is accurate. To meet this commitment you need to ensure that you have good record keeping and ensure records are:

Accurate

Make sure that when you create or update a record the information you are recording is correct and clear. Give patients the opportunity to verify demographics and check records about them and point out any mistakes. Ensure that any factual mistakes are corrected or where appropriate, reported to your manager or a senior clinician.

Up-to-date

Ask patients to confirm their details when attending appointments and ensure changes of address, name, contact details, next of kin details etc are updated as soon as possible.

Record Keeping/Recording Quality Information

Complete, including the NHS Number

Incomplete or inaccurate healthcare information can put patients at risk. For example, the lack of certain information could cause a patient to be given the wrong treatment or advice.

Ensure all patient records include their NHS number; as this helps ensure that the correct record is accessed for the correct patient. All paper forms and supplementary sheets must record the NHS number and be tracked. Remember the Health and Social Care Act supports the use of the NHS number as the unique identifier across Health and Social Care setting to support that continuation of care.

There is also a financial implication of keeping incomplete records.

All treatments carried out by the Trust are coded If these codes are incorrect, or haven't been inputted, then there is no record of them and the organisation will not be paid for activity we are commissioned to undertaken. The Trust may also face allegations of fraudulent behaviour.

Record Keeping/Recording Quality Information

Quick and easy to locate

You need to make sure that records and the information within them can be quickly located when required, as records become more digitised for commissioned activity, staff and corporate records this principle becomes easier to support.

Make sure you comply with any procedures that aim for consistent and standardised filing of records, and for safe and secure records storage areas. If there are no such procedures, speak to your line manager in the first instance, then the Records Manager if necessary about ways of ensuring efficient retrieval of records and the information contained within them.

Free from duplication

Good record keeping should prevent record duplication. Before you create a new record, make sure that one doesn't already exist.

Having more than one record for the same patient/staff member could increase risks, as there may be missing vital information in one record. It would be pot luck which record is accessible in an emergency situation.

Written contemporaneously

Good record keeping requires that information is recorded at the same time an event has occurred or as soon as possible afterwards.

This means that records will be updated live within the digital records whilst the event, care or otherwise, is still fresh in your mind. History sheets should not be completed later and sent for scanning.

Record Keeping/**Good Practice**

There are other issues that you should be aware of and comply with to ensure good record keeping.

Using

When you are responsible for using a record containing personal data you should make sure you comply with the Data Protection legislation and the common law duty of confidentiality, these were covered earlier in this module.

Be aware that individuals are able to gain access to their own personal information under the Data Protection legislation and to other documents under the Freedom of Information Act 2000. Make sure the information you add to records and documents is legible, factual, complete and easy to locate upon request.

Record Keeping/**Good Practice**

Storage

Where paper records remain the key patient record for your service, there needs to be adequate safe secure storage for all the records likely to be created and retained by the Service.

Where your service use digital records you will be responsible for maintaining effective document management within it. If you receive documents by email, ensure you do not retain lots of attachments in your email account, where these relate to patient care, there is need to file in the medical record. Where these contain corporate information, these need to be storage in appropriate systems.

All of these measures will assist you to retrieve files when you need them.

Record Keeping/**Good Practice**

Retention

When a record has achieved its purpose and no longer has any justified use then it is considered closed. After a record has been closed, it should be kept in line with the Record Management NHS Code of Practice retention schedule which will require you to archive or dispose of the record within a certain timescale

You should also regularly review your electronic files and emails and make decisions about whether you need to keep a document or email any longer. If it's no longer needed, consider disposal, either through moving it to an archive file or deletion.

All Staff have a legal and professional obligation to be responsible for any records which they create or use in the performance of their duties.

Any record created by an individual, up to the end of its retention period, is a public record and subject to information requests such as Freedom of Information requests and Subject Access requests.

Record Keeping/What's the best Approach?

Which of the following statements shows the correct approach to managing a record?

a) "We keep track of records from start to finish, and always destroy them when they are no longer needed by the Trust."

b) "We keep track of records from start to finish, and always make decisions on how long a record should be kept, at each point of review, throughout the life of the record."

c) "We keep track of records from start to finish, and always keep all records for at least 100 years in case they are needed in the future."

Record Keeping/What's the best Approach?

This second option is the correct approach.

“We keep track of records from start to finish, and always make decisions on how long a record should be kept, at each point of review, throughout the life of the record.”

The business reasons for keeping records changes over time which emphasises the importance of recognising when a record needs to be reviewed. Guidance on how long a record should be retained and the review considerations are available in the Records Management NHS Code of Practice. The Code also contains guidance on preserving records in an archive

Record Keeping/**Summary**

You have finished this module on good record keeping.

You have looked at:

- Appropriate record keeping
- The importance of accuracy and completeness of records.

Health Records/**Management**

What is a health record?

A clinical history sheet?

An X-Ray?

A Computerised image?

Any of the above?

Health Records/**Management**

What is a health record?

A clinical history sheet?

An X-Ray?

A Computerised image?

Any of the above

A health record is any record that contains information about your physical or mental health condition and is made by or on behalf of health professional involved with your care.

This can be in any format such as paper, computer, or digitised.

This would include for example: -

- Clinical history
- Details of procedures
- X-rays
- Therapy and social work reports

Health Records/**Management**

Other than for clinical/medical purposes, what is a health record used for?

Clinical Audit and Research?

Clinical Audit, Research and Statistical Data?

Medico-Legal?

Medico-Legal, Clinical Audit, Research and Statistical Data?

Health Records/Management

Other than for clinical/medical purposes, what is a health record used for?

Clinical Audit and Research?

Clinical Audit, Research and Statistical Data?

Medico-Legal?

Medico-Legal, Clinical Audit, Research and Statistical Data

The health record can be used for other purposes on the proviso that the patient has been informed. Other purposes are included on the **HOW WE USE YOUR PERSONAL INFORMATION** leaflet**,** which all patients should receive when their appointment or admission details are sent out.
This can be accessed via the Trust website.

Health Records/**Management**

What does a health record NOT contain?

Letters from Solicitors?

Correspondence between Patient and Health Professionals?

Treatment Received?

Patient identifiable information?

Health Records/**Management**

What does a health record NOT contain?

Letters from Solicitors

Correspondence between Patient and Health Professionals?

Treatment Received?

Patient identifiable information?

There should be no document within the health record that does not relate to a patients treatment

Health Records/**Management**

Who is responsible for the health record?

Everyone that handles the health record?

Patient?

Staff?

Medical professional?

Health Records/**Management**

Who is responsible for the health record?

Everyone that handles the health record

Patient?

Staff?

Medical professional?

Everyone that handles the health record is responsible for the safety of the record, this includes the condition of the record, the documents enclosed, the confidentiality of the information is maintained.

Health Records/Management

Responsibilities of those handling health records

- All personal information must be accurate and complete.
- All documentation should be filed within the appropriate section and in the correct order.
- Health Records that are requested, are to be sent in a timely and secure manner
- Health Records **must** be dealt with in a confidential manner.
- Health Records are forwarded to the appropriate department as per Trust guidelines.
- Access to Heath records in digital systems is based on role based access levels.
- All records are **tracked (paper and digital)** and thereby identified by an audit trial.

Health Records/**Management**

Can patient's electronic images be emailed to outside sources?

Yes?

No?

Health Records/**Management**

Can patient's electronic images be emailed to outside sources?

Yes

No?

Yes, however the transfer of personal and personal sensitive information must only occur when it can be legally justified and must be encrypted during transfer. Should you need to electronically transfer patient information please contact the IT to ensure you have the appropriate settings and functionality available on your computer/laptop.

Health Records/**Management**

If you are transferring copies of a patient's health record outside the Trust what is the correct postal process to follow:

By standard post in an envelope?

By recorded delivery in an envelope?

By special delivery in a secure transport bag?

Health Records/Management

If you are transferring copies of a patient's health record outside the Trust what is the correct postal process to follow:

By standard post in an envelope?

By recorded delivery in an envelope?

By special delivery in a secure transport bag

When not sealed and using Trust transport then Special Delivery must be used.

REMEMBER A WELL MAINTAINED HEALTH RECORD WILL REFLECT ON THE TRUST!

LOOK AFTER THEM!

Information Security/Overview

Spot the Security Breach!

In the Trust, you are responsible for keeping patient information safe and secure. Can you spot the potential security breaches in each of these situations?

“I really need to get on top of updating my patient records. I’ll just pop them onto this memory stick to

Information Security/Overview

Spot the Security Breach!

In the Trust, you are responsible for keeping patient information safe and secure. Can you spot the potential security breaches in each of these situations?
take home with me."

Information Security/Overview

Spot the Security Breach!

In the Trust, you are responsible for keeping patient information safe and secure. Can you spot the potential security breaches in each of these situations?

"I really need to get on top of updating my patient records. I'll just pop them onto this memory stick to take home with me."

The doctor is transferring patient information to a portable device to take home with him!

The risk of theft of any portable media is high. But due to their size, memory sticks are at a higher risk of being misplaced. If you have been authorised to use a memory stick to transport patient information it must be encrypted

Information Security/Overview

Spot the Security Breach!

In the Trust, you are responsible for keeping patient information safe and secure. Can you spot the potential security breaches in each of these situations?

"Can I borrow your security pass for a few minutes? I left mine at home!"

Angelique has forgotten her door pass. She needs to get something from the stock room so asks her colleague to borrow her pass.

Information Security/Overview

Spot the Security Breach!

In the Trust, you are responsible for keeping patient information safe and secure. Can you spot the potential security breaches in each of these situations?

"Can I borrow your security pass for a few minutes? I left mine at home!"

Angelique has forgotten her door pass. She needs to get something from the stock room so asks her colleague to borrow her pass.

Do not lend out your security pass to anyone else – not even to close colleagues. Your pass is intended for you and your use only. You have no control over the security consequences if it gets into the wrong hands, but you will be identified by any audit trail as the individual who accessed the system, room or area.

All staff should feel empowered to challenge strangers in an area, who are not carrying any visible identification on them.

Information Security/Overview

Spot the Security Breach!

In the Trust, you are responsible for keeping patient information safe and secure. Can you spot the potential security breaches in each of these situations?

"My password is my girlfriend's name. It's easy for me to remember that way!"

Information Security/Overview

Spot the Security Breach!

In the Trust, you are responsible for keeping patient information safe and secure. Can you spot the potential security breaches in each of these situations?

"My password is my girlfriend's name. It's easy for me to remember that way!"

David has chosen a password he can remember. What he doesn't realise is that anyone who knows him could easily guess it.

Always select a password that cannot be found out by anyone else.

Password standards mean that our passwords need to include Upper case, Lower case a number and a character. For example "Jennifer" could become "Jen2!fer"

All Information Asset system owners should ensure that systems settings mandate and force password strength and changes at appropriate intervals.

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Information should be kept safe and protected at all stages during which it is held by the Trust. You looked at why information must be protected in confidentiality. Information security is more concerned with how information is protected, for example, using passwords, locks and security passes. Good information underpins good care. Is supported by

confidentiality

Integrity

Accessibility

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 unmodified
Availability is about information being there when it is needed to support care

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Scenario

- Jane falls badly and hurts her leg.
- The paramedics ask Jane for her details and whether she is allergic to any medications but Jane isn't sure.
- The paramedics attempt to access Jane's Summary Care Record, [**Confidentiality** – the Paramedics have a legitmate need to see the record.] But there is a telephone network outage preventing access.
- The paramedics administer morphine, but Jane is allergic – a fact held on her record – and goes into anaphylactic shock. [**Integrity** – the record is correct and unmodified but was not available.]
- In hospital she is kept in intensive care. In this case the lack of information **Availability** has had a direct impact on the care of this patient

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

A reliable record

Information should be a reliable presentation of what was recorded, so that people know they can make decisions based on it. It is important that the information we use is a reliable presentation of what was recorded, particularly personal information as this is used to provide care and treatment. Implementing information security measures helps us to ensure that information created or used is accurate, complete and not tampered with.

Available to authorised people

Information should be available to those authorised to see it at the time they need it.

The information security measures put in place must ensure those authorised to use information have access to it where and when it's needed, within solutions that provide for audit trails into any potential inappropriate access.

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

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

Information Security/Good Practice

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security- 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.

Information Security/Good Practice

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security- Fake IT Dept

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.

Remember the ICT department or provider will not need to ask these types of questions

Do not provide details, contact the Service Desk to report instances where this occurs, to facilitate central action to block or cascade warning messages to staff.

Information Security/Good Practice

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security- Fake IT Dept

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.

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security 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 it's from a colleague - double check by phoning the colleague.
- Do not open links or attachments in unsolicited emails.

Report suspicious emails to the IT department or provider.

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security - 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 IT department
- 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 IT department or provider – the Trust processes for dealing with spam will be inacted

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security - Malware

- Malicious software (malware) can:
  - Be on your computer and evade detection.
  - Make your computer run slowly or perform in unusual ways.
- The IT 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

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security - 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’."

Information Security/Good Practice

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security - 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 the Trust's processes for secure disposal
- Follow the Trust's processes when moving location
-

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security - Clear working environment

Follow your organisation's clear desk policy.

Do not leave information in unsecure locations.

Always lock screens when not in use

Be vigilant with diaries/register books etc

Review content of white boards and notice boards

Having a clear desk means reduced potential for leaving sensitive information unattended, reducing the risk of a breach.

Information Security/Good Practice

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Avoiding threats to data security – threat types

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	

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Stop others from viewing the information

Keep electronic records password protected

Choose effective passwords

Avoid inappropriate disclosures of information

Ensure the premises are secure

Seek advice from your IG Lead

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Stop others from viewing the information

Don't leave paper records lying around; lock them away when they're not being used.

Return paper records to the correct storage area when no longer required so that they are available if needed by someone else

Secure the screen (Ctrl, Alt, Delete) (Windows,L) when you need to walk away from the PC when logged into patient information systems.

If you see a colleague's device open and unlocked, lock it for them and gently remind them to do so in future

Consider siting screens at angles to prevent patient/visitor visibility in areas such as reception

Never share passwords, or allow others to use your login.

As an Information Asset Owner, ensure you have starter/leavers processes in place and run appropriate access audits.

Keep electronic records password protected

Choose effective passwords

Avoid inappropriate disclosures of information

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Ensure the premises are secure

Seek advice from your IG Lead

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Keep electronic records password protected

Activate the secure screen saver using (Ctrl, Alt, Delete) or (Windows,L) to prevent unauthorised access to electronic records if you have to leave your computer unattended.

Log out and switch off your computer at the end of each session.

Do not share your password with colleagues or allow other to use your account

Regularly change your password, maintaining a high strength password.

Trust standards dictate that only encrypted Laptops and memory sticks can be used.

Choose effective passwords

Avoid inappropriate disclosures of information

Ensure the premises are secure

Seek advice from your IG Lead

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Stop others from viewing the information

Keep electronic records password protected

Choose effective passwords

Choose a good password of at least 8 characters long, with a mixture of letters, numbers and symbols.

Keep passwords secret and your smartcard safe.

Avoid inappropriate disclosures of information

Ensure the premises are secure

Seek advice from your IG Lead

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Stop others from viewing the information

Keep electronic records password protected

Choose effective passwords

Avoid inappropriate disclosures of information

Make sure you don't discuss sensitive information in inappropriate venues, e.g. public areas of the Trust.

When you take phone calls ask patients to confirm personal information to you rather than you reading their details out loud.

Be careful when selecting email address's, do not send to a whole distribution list, only those who need to see the data.

Never disclose patient information through social media websites.

Ensure the premises are secure

Seek advice from your IG Lead

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Stop others from viewing the information

Keep electronic records password protected

Choose effective passwords

Avoid inappropriate disclosures of information

Ensure the premises are secure

Don't leave key coded doors propped open.

If you're the last to leave the building at the end of the working day, make sure windows and doors are locked. If there is a burglar alarm make sure it is turned on.

Seek advice from your IG Lead

Information Security/**Good Practice**

What measures should you take to ensure that information is appropriately protected so that access is controlled but the information is available to those authorised to use it? Click each option in turn to read more.

Stop others from viewing the information

Keep electronic records password protected

Choose effective passwords

Avoid inappropriate disclosures of information

Ensure the premises are secure

Seek advice from your IG Lead

Make sure you seek advice from the Information Governance Manager or Head of Information Assurance when faced with an unexpected situation.

If you discover an actual or potential breach of information security, such as missing, lost, damaged or stolen information and equipment make sure you report through DATIX

Information Security/Portable Equipment and Removable Media

How else can you ensure information remains secure?

- Only transfer personal information to removable media such as CDs, DVDs and memory stick if you have been authorised to do so, then using the minimum data required
- Do not plug in any non-approved devices to charge via a USB cable
- All removable media must be encrypted
- Look after portable equipment such as laptops, PDAs, tablet and memory sticks.
- All portable equipment must be encrypted
- If you're travelling with them ensure you keep them within your sight at all times. Where possible attach a memory stick to a key ring.

Keep regular backups of the data stored on digital assets – store appropriately, in line with Trust policy

For more information on laptop security, please see the IG policies or contact the Information Security team.

Information Security/**Password Management**

David chose a password that was easy for anyone who knew him to guess. The password you choose should be memorable but hard to guess.

Consider the passwords below, which of these would be the most effective?

18feb1980

Reds

Dk9+jtb3sH*nw26w

#5~Lp4Y

Information Security/**Password Management**

David chose a password that was easy for anyone who knew him to guess. The password you choose should be memorable but hard to guess.

Consider the passwords below, which of these would be the most effective?

18feb1980

Reds

Dk9+jtb3sH*nw26w

#5~Lp4YAF

The first two are too easy to break.

Information Security/**Password Management**

David chose a password that was easy for anyone who knew him to guess. The password you choose should be memorable but hard to guess.

Consider the passwords below, which of these would be the most effective?

18feb1980

Reds

Dk9+jtb3sH*nw26w

#5~Lp4YAF

The third one would be difficult to remember without writing down.

Information Security/**Password Management**

David chose a password that was easy for anyone who knew him to guess. The password you choose should be memorable but hard to guess.

Consider the passwords below, which of these would be the most effective?

18feb1980

Reds

Dk9+jtb3sH*nw26w

#5~Lp4YAF

The fourth option is a memorable password for David because it is based on one of his favourite songs, “I say a little prayer for you” by Aretha Franklin.

It uses a mixture of at least eight letters, numbers and special characters.

Information Security/

Personal and Acceptable use of IT Equipment

Personal and acceptable use of the internet and email is permitted within the Trust. But what do you think is acceptable and personal use, and when is it considered excessive?

Acceptable use

- Sending, displaying or knowingly accessing offensive material is a breach of the acceptable use policy.
- You should not commit to email anything which you would be unhappy to sign your name to in print.
- Any non-work related email or documents, e.g. private emails, should be stored in your email account or network folder clearly marked as ‘Personal’.
- The Trust has internet filters in place to help block offensive sites, but if you do come across any while doing legitimate work you should inform the Information Security team.
- If you suspect that a staff member, patient or relative has been accessing sites on the in internet that are criminal or offensive in nature you must discuss your concerns with your Line Manager, Information Governance or Human Resources.

Information Security/

Personal and Acceptable use of IT Equipment

Personal use

- IT facilities such as the internet and email have been provided by the Trust primarily for business purposes.
- The Trust permits limited personal use of these facilities

Excessive personal use

- Excessive personal use or inappropriate use of the IT systems is a disciplinary offence.
- The Trust has both email, internet and Social Media policies that contain explicit details of what is acceptable, excessive or inappropriate use. Do read the policies they cover such things as accessing or downloading pornographic images, or carrying on a business using the organisation's email and other IT facilities or sending harassing or offensive emails, etc.

Information Security/**Appropriate Use of Email**

Every morning David's inbox is full of Spam. What should he do with these emails?

a) Reply and tell them to stop sending them

b) File them in a folder marked 'Spam'

c) Delete them without opening

d) Forward them if they look interesting

Information Security/Appropriate Use of Email

Delete them without opening.

Never keep junk emails. Never forward them to others or even reply – delete them! The best way of doing this is to highlight the email, hold the Shift key and press delete.

If the email contains a link to an unsubscribe facility, do not click on it. It just confirms that yours is a valid email address and will result in you receiving even more junk mail!

If you receive frequent and large amounts of junk emails discuss this with the Service desk, as they may be able to help you to reduce the occurrence.

Do always look at attachments before forwarding them out of the organisation. If they contain personal information should you be sending it? If so are you sending it securely?

Information Security/

Audit Trails and Reporting Security Breaches

Why is it important that everything you do on a computer, including emails and internet use, can be tracked?

- Where breaches of security, the law or the acceptable use policy are suspected, this tracked data can be used to aid an investigation.

- Any incident, however small, wastes time and often requires work to be repeated. It also poses a risk to individuals or the organisation.

- We can make improvements to security by reporting any breaches through the Datix Adverse Incident Reporting system

Information Security/**Installing software**

Dr Jones has a favourite programme he uses for index cataloguing his research papers. He downloads the software from the internet onto his computer. Should he do this?

Information Security/**Installing software**

Dr Jones has a favourite programme he uses for index cataloguing his research papers. He downloads the software from the internet onto his computer. Should he do this?

No!

You should never use/download software that hasn't been authorised by the Trust on to your work computer. There are two main reasons why you should never do this;

- First, you risk infecting your computer, other computers and the network from malicious code embedded in the software

- Second, there are licensing issues. The Trust has to pay for a license for software used on its network.

If software is required this should be discussed with the Head of Service and IT before purchase

Information Security/

Malicious Code and Unauthorised Software

So, by installing software yourself, you risk infecting the network with malicious code and potentially creating licensing issues for the organisation. Here is some advice about the issues and what you can do to counter the risk of either occurring.

Malicious code

Malicious code includes computer viruses and spyware, and the effects will vary depending on which you have downloaded. Some malicious code will just waste time while another can destroy data or even allow another user to gain access to your computer. Email attachments you receive may also contain malicious code.

To combat some malicious code, the Trust has an anti-virus system that will catch most incoming viruses on emails. You can help by being extremely cautious of opening email attachments from people you don't know.

Remember: Do not download software from the internet, from free CDs etc, unless you have been authorised to do so. If in doubt get advice from your IM&T Service Desk or the Information Security team

Information Security/

Malicious Code and Unauthorised Software

So, by installing software yourself, you risk infecting the network with malicious code and potentially creating licensing issues for the organisation. Here is some advice about the issues and what you can do to counter the risk of either occurring.

Unlicensed software

Software includes any programs and games you download from the internet, CD or any other storage media.

The Trust has processes regarding the installation of such software, and if you install software without authorisation this process is bypassed. You then put the Trust at risk of legal action from the owner of the software.

Any ‘free’ software could be an illegal copy, or it could be trial software with an expiry date. Even if neither of these things apply, the software is likely to be for single personal use and require a licence for corporate use.

Remember: Do not install software from the internet, from free CDs etc, unless you have been authorised to do so.

Information Security/**Securing Access to Information**

Who do you think is responsible for securing information in your workplace?

a) Senior Management staff

b) Receptionists

c) Nurses

d) Doctors

Information Security/Securing Access to Information

Feedback

It is **everyone's** duty to secure information at work, no matter what your role.

This means you are responsible for reporting any known or suspected breaches in security, as well as any weaknesses in security measures. Make sure you know how to contact the IG Lead or Information Security Officer.

Information Security/Securing Access to Information

Question

Doug comes across a cage of documents in a corridor. He makes a mental note of this but by the time he has got back to the ward he has forgotten.

What should Doug have done?

Answer

If the documents are patient information then this is a potential security risk. He needs to immediately contact the information governance department or his manager so that the documents can be taken to a place of safety and examined. Recording the cage onto the DATIX system, will push messages to the relevant staff to address mitigation to occur.

Information Security/Securing Access to Information

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

- **Doors**: Nearly every door 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.
- Where standards of physical security fall to this level within a working area, he can potentially come and go as he pleases…perhaps next week.

We are all accountable for Information Security standards in our working area

Information Security/Securing Access to Information

Miss Broom is waiting to receive information from her clinician. 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 service 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. A DATIX incident report is raised to register the data breach – this notifies relevant staff of the incident for an investigation to be completed

Consequences – The Trust 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 Trust 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 Trust

Information Security/Securing Access to Information

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

Information Security/Securing Access to Information

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.

Good Practice

Confirm the enquirer's name, job title and organisation.
Confirm the reason for requesting information 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.

Information Security/Securing Access to Information

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.

Information Security/**Summary**

Here are the key steps you can take to secure access to information, in and out of the workplace.

Protect patient information and other sensitive information from unauthorised access, destruction or loss by:

- Ensuring paper and electronic records are secure.
- Choosing an effective password.
- Avoiding inappropriate disclosures.
- Ensuring that Trust buildings are secure.
- Deleting spam without opening it.
- Never downloading software unless authorised.
- Using IT equipment responsibly.
- Knowing how to report suspected and actual breaches of security.

Remember, **everyone** is responsible for securing information in the workplace. See the Trust's IG policy specific to your area.

Summary

This module has given an overview of Information Governance (IG).

IG allows the Trust & other organisations, together with individuals, to ensure information is processed legally, securely, efficiently and effectively. IG applies to all the types of information which the Trust may process, but the rules may differ according to the type of information concerned.

Summary/**Responsibilities**

Remind yourself of the answers to these questions.

1. Who is responsible?

Everyone is responsible for IG and for:

- Providing a confidential service to patients, sharing information lawfully and appropriately
- Recording information accurately and ensuring it is accessible when needed
- Ensuring that information is held securely
- Processing information in accordance with the ‘data protection rules’ and respecting the rights of individuals
- Complying with Freedom of Information requirements.

Summary/**Responsibilities**

Remind yourself of the answers to these questions.

2. Where can I get advice about confidentiality?

If you need any advice about confidentiality issues, you should refer to the:

- IG Lead, Caldicott , Data Protection Officer or Senior Information Risk Officer
- Care Record Guarantee which sets out our commitments to patients
- The six Caldicott principles for handling patient information
- Confidentiality NHS Code of Practice

Summary/**Responsibilities**

Remind yourself of the answers to these questions.

3. How do I comply with good record keeping principles?

When you enter information into a record or document, ensure it is:

- Accurate
- Legible
- Written at the time an event occurred
- only use your own log in/password to enter details into a computer record

When you are responsible for storage of files or documents, make sure you use a logical naming and filing system so that they are easy to locate and retrieve.

For more in-depth information about records management principles, see the Records Management NHS Code of Practice at the link below
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

Summary/**Responsibilities**

How can I keep information secure?

Look at your organisation's Information Governance and IT policies specific to your area for the security standards you need to meet. In general you should:

- Choose a secure password, and keep it private
- Lock away files when they are not in use
- Delete spam emails without opening them
- Never use unauthorised software.

Summary/**Relevant Legislation**

The General Data Protection Regulations and supporting Data Protection Bill

This legislation states that information should be:

- Processed lawfully, fairly and in a transparent manner
- Processed for specified, explicit and legitimate purposes
- Adequate, relevant and not excessive
- Accurate and kept up-to-date
- Not kept for longer than necessary
- Processed in accordance with rights of data subject
- Protected by appropriate security

Summary/Relevant Legislation

The Freedom of Information Act 2000

This Act gives the public the right to request any information held by any type of public authority or healthcare organisation.

These requests must be made in writing

Organisations must respond within 20 working days

Each organisation must have an FOI lead who is trained in dealing with these requests.

If your job requires you to deal with FOI requests you are advised to participate in a more advanced training package.

Summary/Links to Further Information

Trust IG Policies (needs PAT link)

http://intranet.srht.nhs.uk/policies-resources/trust-policy-documents/departments/imt/

The Information Commissioners Office

http://www.ico.gov.uk/

The NHS Confidentiality Code of Practice

http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550

Records Management Code of Practice for Health and Social Care 2016

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Information security management NHS code of practice

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/information-security-management-nhs-code-of-practice