Information Governance

Level 1 - All staff involved in routine access to information Core Skills Reader

Introduction to the Core Skills

The Core Skills standardises the training for 10 subjects commonly delivered as part of statutory and mandatory training requirements for health and social care organisations.

For each subject a set of learning of outcomes has been agreed nationally and is set out in the UK Core Skills and Training Framework (a copy of the framework is available on the Skills for Health website: www.skillsforhealth.org.uk/)

The learning outcomes specify what needs to be covered in the training for each Core Skills subject, this ensure a quality standard is set and provides clear guidance for organisations to deliver against these requirements as well as recognise the equivalent training delivered externally. This allows for Core Skills training to be portable between organisations and prevents the needless waste and duplication of statutory and mandatory training where is not required.

To aid organisations in the delivery of the Core Skills subjects, these education resources have been developed that are aligned to the learning outcomes in the UK framework. Organisations have the flexibility to deliver these resources in a variety of formats as well as adapting them to add localised content alongside the Core Skills Materials.

If you require any further information about the Core Skills, in the first instance please contact the Learning and Development Lead in your organisation.

Introduction to Information Governance

This reader covers the Core Skills learning outcomes for Information Governance.

This resource has been designed to cover induction level training and addresses the key principles in Information Governance for individuals involved in routine access to personal healthcare information and records.

This is likely to be a minimum requirement for all staff working in a health setting and specific staff groups will require additional training dependent upon their role.

It is anticipated that it will take you approximately 15-30mins to complete this reader. Current national guidelines recommend that Information Governance is repeated every year.

What you will learn in this Reader

The objectives below covered by this reader are aligned to the Learning Outcomes for Health, Safety and Welfare in the Core Skills and Training Framework.

1. Principles of Information Governance and their application to health and social care organisations
2. Accessing Information Governance resources including national legislation, guidance and local policies & procedures
3. Health and social care organisation's responsibilities
4. Protection of an individual's confidentiality and the Caldicott Principles
5. How to practice and promote a confidential service
6. Principles of ensuring and maintaining good client records
7. Recognising / responding to Freedom of Information requests
8. Keeping Information Secure

What is Information Governance?

> ***Information Governance is about how health and social care organisations and their employees must handle sensitive information***

Information Governance is about dealing correctly with all the different ways that both employees and organisations handle information. It allows for information to be processed legally, securely, efficiently and effectively.

Good information governance practice will hopefully ensure the necessary safeguards for appropriate use of patient and service user's personal and sensitive information as well as the health and social care organisations records.

A balance is needed between the protection of the patient/ service users' personal and particularly sensitive information and the need for appropriate sharing of information to ensure high quality care delivery.

Information Governance Framework

The Information Governance Framework for health and social care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that these standards are clearly defined and met
NHS Connecting for Health (2013)

The central focus of information governance is how personal and sensitive information about patients and service users is managed from conception to destruction.

The principles and framework for information governance are applied in the same way to:

- NHS Trusts (Acute, Paediatric, Mental Health, Community)
- Foundation Trusts
- Independent sector NHS providers (through contractual arrangements)

What is Information?

Type of Information	Examples
Personal	▪ Name ▪ Address ▪ Date of Birth ▪ Next of Kin
Sensitive	▪ Diagnosis ▪ Illness & Disorders ▪ Sexual Orientation ▪ Ethnicity
Corporate	▪ Minutes of Meetings ▪ Employee Details ▪ Financial Information

Can you think of other examples?
Where do you think this kind of information can be found?

For example; health records, case notes, doctor/nurse/paramedic notes, prescriptions, databases, post it notes, etc.

It is important to remember that organisations are also responsible for their employees' personal data. For example, HR files, interview notes, disciplinary procedures and notes.

Corporate or organisation information may include details of estates contracts, minutes of meetings, etc. Notes that people take down at meetings in the wrong hands could be very damaging.

Why is Information Governance so Important?

Area	Examples
For patients and service users	▪ Information is critical for safe, timely and effective care ▪ Information is sensitive ▪ Excellent healthcare is built on a foundation of confidence & trust
For an employee	▪ Sensitive information ▪ Ethical and legal responsibility of every employee ▪ Information must be: accessed, used & shared appropriately
For a health or social care organisation	▪ Ethical and legal responsibility of every organisation ▪ Breaches of confidentiality costs money and reputation

Information Governance is important both ethically and legally. This is highlighted in the table above. Can you think of any other examples?

There are many laws, principles, policies and procedures that have been developed in order to protect individuals including patients, service users and employees. If followed correctly, these will also guide and protect public organisations.

The NHS Chief Executive has made it clear that ultimate responsibility for information governance in the NHS rests with the board of each NHS organisation. Each organisation is required to have a board-level Senior Information Risk Owner (SIRO) and a Senior Information Asset Owner should be designated for every separate database or other major information asset.

The SIRO is:

- Accountable
- Fosters a culture for protecting and using data
- Provides a focal point for managing information risks and incidents
- Is concerned with the management of all information assets

The SIRO's role is different to the Caldicott Guardian (see page 11). However both roles have to work closely and consult where appropriate when conducting information risk reviews for assets which comprise or contain patient information.

Information Governance requirements for health and social care organisations

Clear requirements for the handling of information have been developed by the Department of Health and are set out in the **HORUS** model shown below

All information must be:

H eld securely and confidentially
O btained fairly and efficiently
R ecorded accurately and reliably
U sed effectively and ethically
S hared appropriately and lawfully

The Law and Information Governance

Information Governance is covered by both common law and set pieces of legislation or Acts of Parliament.

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The key pieces of law are summarises below (For more information select each sub heading to open the relevant web link):

- **Common Law Duty of Confidentiality**:
  (Taken from the Department of Health 2013)
  The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

  In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

  There are 3 circumstances where making disclosure of confidential information lawful. These are:

  - Where the individual to whom the information relates has consented
  - Where disclosure is in the public interest
  - Where there is a legal duty to do so, for example a court order

- **Computer Misuse Act 1990**
  It is an offence to access or attempt to access computer information without appropriate authorisation.

- **Data Protection Act 1998**

  The Data Protection Act controls how an individual's personal information is used by organisations including health and social care organisations. Everyone who is responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

  - Used fairly and lawfully
  - Used for limited, specifically stated purposes
  - Used in a way that is adequate, relevant and not excessive
  - Accurate
  - Kept for no longer than is absolutely necessary
  - Handled according to people's data protection rights
  - Kept safe and secure
  - Not transferred outside the UK without adequate protection

  There is stronger legal protection for more sensitive information, such as:

  - Ethnic background
  - Political opinions
  - Religious beliefs
  - Health
  - Sexual health
  - Criminal records

- **The Human Rights Act 1998**

  The Human Rights Act 1998 (also known as the Act or the HRA) came into force in the United Kingdom in October 2000. It is composed of a series of sections that have the effect of codifying the protections in the European Convention on Human Rights into UK law.

  All public bodies (such as courts, police, local governments, hospitals, publicly funded schools, and others) and other bodies carrying out public functions have to comply with the Convention rights. This means, among other things, that individuals can take human rights cases to domestic courts; they no longer have to go to Strasbourg to argue their case in the European Court of Human Rights.

The Act sets out the fundamental rights and freedoms that individuals in the UK have access to.

- **Freedom of Information Act 2000**
  The Freedom of Information Act gives individual the right to ask any public sector organisation including health and social care organisations for all the recorded information they have on any subject.

  Anyone can make a request for information – there are no restrictions on your age, nationality or where you live. A request will be handled under the Data Protection Act if they ask for information about themselves.

Standards, Policies & Codes of Practice

To support the law and legislation in place there are a number of national Standards, Policies and Codes of Practice that apply the law in context and provide guidance to organisations and individuals to help them adopt and follow best practice.
For more information select each sub heading to open the relevant web link.

- **Information Security Standards – ISO/IEC 17799: 2005 and IS Management NHS Code of Practice**
- **The NHS Confidentiality Code of Practice**
- **Records Management Code of Practice for Health and Social Care 2016**
- **Information Quality Assurance**

Always follow the Caldicott Principles

To maintain levels of confidentiality in the NHS, the Department of Health commissioned the Caldicott Report in 1997. One of the main recommendations was that staff justify every use of confidential information and test it against the 7 principles shown on the next page:

- Justify the purpose of using confidential information
- Only use it when absolutely necessary
- Use the minimum information required
- Allow access on a strict need-to-know basis
- Always understand your responsibility
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

You **MUST NOT** disclose confidential information if you are unsure or unable to apply any of the principles above.

Caldicott Guardians

To ensure the Caldicott Principles are applied and adhered to, the report also called for Caldicott Guardians to be appointed in every NHS Trust.

The Caldicott Guardian should be a senior person in the organisation, usually at board level. For example, the Director of HR, Medical Director or Director of Nursing are all senior positions that would be suitable to be the Caldicott Guardian for an organisation.

They are responsible for reviewing, overseeing and agreeing policies that govern the protection of patient and personal information; along with ensuring compliance by the organisation to the Caldicott Principles.

Find out who the Caldicott Guardian is in your organisation.

Subject Access Requests

Individuals have the right to access sensitive information including paper, computer records and other related information

A subject access request is a request from an individual who wants to view the personal information that is held about them.

Patients and service users may request to see their health and social care records, while employees may request to see their HR records. There is a formal process which organisations should have in place to provide this information.

Requests should be in writing and compiled with by the organisation within no more than 40 days, but ideally information should be provided within 21 days.

Make sure you know the person in your organisation that is responsible for subject access requests.

What is a Freedom of Information (FOI) Request?

It’s important to understand the difference between the Data Protection Act and the Freedom of Information Act.

Individuals have the right of access to information about them ('personal data'), held on computer or in paper files, under the Data Protection Act 1998.

The Freedom of Information Act extends this right to allow individuals the right to access / view all non-personal public authority information upon request, which must be made in writing.

Types of information that can be requested include minutes of meetings, work emails, handover notes, off duty rotas, etc. The Act does, however, set out some exemptions to this right, for example:

- The information can be easily obtained from elsewhere
- The information has already been published or there are plans to do so
- It is confidential information
- It is personal information (either about the applicant or someone else)

The information must be supplied if it exists and an exemption cannot be applied. In general, an organisation needs to respond to a FOI request within 20 working days. There is also a duty on public authorities to provide advice or assistance to anyone seeking information (for example in order to explain what is readily available or to clarify what is wanted).

Organisations could face financial penalties if they don't comply or if they are in breach of the Act. It is because of this that any FOI requests received should be directed to the FOI Lead to decide how best to respond.

- Looking at the 2 examples below, can you recognise which one is a FOI request and explain why?

Duty of Confidence

You have a legal duty
to protect and maintain confidentiality

This is called the Duty of Confidence, and will be reflected in your contract of employment and code of professional conduct. Duty of Confidence applies to when sensitive 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 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 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.

You need to be careful and cautious when dealing with requests for information, particularly over the telephone. Is the request genuine or is the information trying to be obtained under false pretences?

Requests need to be verified and if possible obtained in writing.

If you are unsure, don’t disclose

Instead refer the matter to your manager or the Caldicott Guardian, who is responsible for ensuring confidentiality in your organisation.

Good Quality Record Keeping

Good quality record keeping is essential. Poor quality records or inaccurate information can place patients & service users, employees' and organisations at risk. Ask yourself the following:

- Does a record already exist?
  Duplicated records create a risk. One set may not be up to date. Crucial information could be missed.
- Are they clear, factual, accurate & complete?
  Consider the consequences if information is missing or misunderstood
- Can everybody else read them?
  They need to be legible, particularly hand written records
- How long does it take?
  Complete them quickly!
- Are they dated, timed and signed?
  Provide an auditable history of interventions
- Is the information up-to-date?
  For example have personal details changed?
- Are they stored safely?
  Need to maintain confidentiality
- How long the records should be retained for?
  If no longer needed, records should be disposed of safely
- Do you know how to correctly delete records?
  Refer to your organisation's policy and procedures

Good record keeping is also essential in case of requests under the Data Protection Act or the Freedom of Information Act.

For more information regarding good quality record keeping refer to your Professional Standards of Practice and the Records Management: NHS Code of Practice

Information Security

Information security is about making sure information is:

- Protected and secure
- Reliable
- Available to authorised users only

It is an important element of information governance and is often a contemporary topic, with significant breeches by high profile public figures highlighted regularly in the news.

Concerns about public sector data protection have resulted in the Government directing a range of standards for managing information risk. These standards are reflected within the NHS Information Governance Toolkit which can be accessed from: https://www.igt.hscic.gov.uk/

Remember simple actions will keep information secure and confidential. However, it is also simple and thoughtless actions which often result in breeches of confidentiality. It is your responsibility to ensure:

- Records are correctly stored
- Passwords are kept secure
- Report inappropriate disclosures
- Delete spam mail without opening
- You don’t download unauthorised software
- You use IT equipment correctly

It is important you know and understand the information security arrangements, policy and procedure in your organisation, and remember:

- Any breaches of data security, no matter how small, must be reported!
- Organisations monitor the access and use of information and systems and failure to ensure your legal responsibility or trust policy could result in serious disciplinary and legal action.

Your Responsibilities

Remember your responsibilities, summarised in the DO and DON'T tables below:

DO

- Protect an individual's information
- Be aware of national & local information, Policy & Procedures
- Inform patients how information is used and when it may be disclosed
- Help to improve the way organisation protects information
- Report any suspected or actual breaches of information security
- Seek advice from the appropriate leads if you have any Information Governance concerns

DON'T

- Send confidential, person-identifiable data without applying the required encryption/security measures
- Store Personal/Sensitive information on unencrypted and unauthorised portable devices
- Disclose confidential information with unauthorised people
- Leave person-identifiable data (PID) unattended or in vehicles
- Access inappropriate websites
- Use an organisation's equipment or information to promote private business or for financial gain

Useful Sources of Information and Links

For further advice contact the local Information Governance Manager or Lead in your organisation.

Useful Links:

- Information Commissioners Office www.ico.org.uk/
- Connecting for Health Toolkit www.igt.hscic.gov.uk/