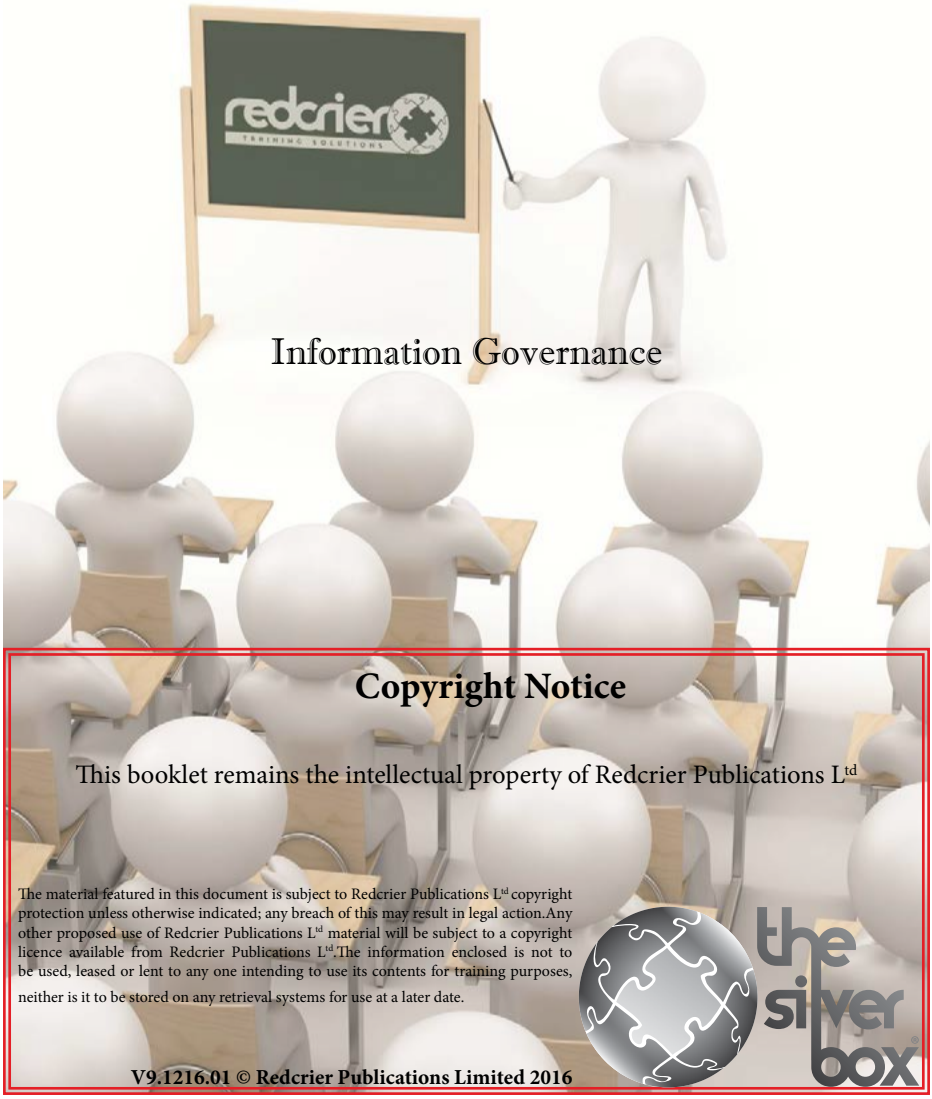

Information Governance

Copyright Notice

Information Governance

Information Governance (IG) is a term used to describe the systems and protocols in the storing, handling and use of personal information held about an individual. Any person responsible for the holding of personal data has a statutory duty to ensure it is held securely, that it is relevant and that it is used for the purpose for which it is being held.

Protection of personal and sensitive personal data is provided through the Data Protection Act 1998.

Personal data is data held which relates to a living person who can:

A. Be identified from the data.

B. Be identified from the data or other information either in possession, or likely to come into possession of the data controller. This may include expression of opinion or indication of intentions of the data controller or other persons in connection with the person whose data is being held.

Sensitive personal data.

The Data Protection Act 1998 defines sensitive personal data as consisting of information which reveals the following information about them:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- The commission or alleged commission of any offence.
- Any proceedings for any offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings.

Information Governance

Confidentiality.

Confidentiality can be defined as:

"Entrusted with private or restricted information".

Your organisation should have a confidentiality policy available to everyone.

Confidentiality is an essential principle in the provision of health and social care. Health and social care professionals are entrusted with personal data relevant to those in their care; such data must be safeguarded against misuse and abuse. In health and social care personal information is passed, routinely, to those authorised care workers involved in the care of the individual. This requires a bond of trust to exist between all parties involved. As a principle, confidentiality is not absolute. In cases where safeguarding concerns are raised, confidentiality cannot be promised. Information may be shared with agencies or individuals not involved in their direct care i.e. police and social services.

Confidentiality must not be put before the safety of individuals.

The Caldicott Principles.

These principles relate to the findings of Dame Fiona Caldicott, who was commissioned by the Chief Medical Officer to look into the concerns of how patient information was being used in the NHS.

The Caldicott Principles:

1. **Justify the purpose(s).**

   The proposed use or transfer of patient identifiable information should be clearly defined and regularly reviewed, by an appropriate person.

2. **Don't use patient identifiable information unless it is necessary.**

   The need for patients to be identified should be considered at each stage and for each purpose.

3. **Use the minimum necessary patient-identifiable information.**

   The extent of personal information required should be considered and justified for each function to be carried out.

4. **Access to patient identifiable information should be on a strict need-to-know basis.**

   Only those individuals who need access to patient identifiable information should have access to it and then only information relevant to them.

5. **Everyone with access to patient identifiable information should be aware of their responsibilities.**

   Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law.**

   Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

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

   Professionals, should in the patient's interest share information within this framework. Official policies should support them doing so.

Security of information.

Security describes the condition that protects safety and guards against theft. Personal information is a valuable commodity used correctly it can be of great benefit to the person, misuse or abuse may have the opposite effect and may place the person at risk of harm or exploitation (see Redcrier Safeguarding Manual). Protecting information is everyone's responsibility.

Confidentiality - secured against unauthorised access.

Integrity - safeguarded against unauthorised modification.

Availability - accessible to authorised users at times when required.

Today, much of the stored personal information is held electronically. Steps must be taken to ensure the safety of any personal information held on electronic devices. Measures which can be taken to protect information on electronic devices may include:

- Switch off or log out of the device when not in use. This includes peripheral equipment such as printers and scanners.
- Only authorised persons to use data storage devices.
- No illegal copies of software to be made from the system.
- Never leave portable devices unattended.
- Ensure personal information is saved to the server and not the C:\Drive.

- Memory sticks and CDs, or any other storage medium, do not contain personal information.
- Position monitors so they cannot be overviewed by unauthorised persons.

When using passwords:

- Do not tell anyone else your password – ever.
- Do not write passwords down.
- Always log out when you have finished inputting or reviewing data.
- Be aware who is around when inputting your password. Can they observe your screen or key strokes?
- Avoid creating a weak, or easily guessed, password e.g. password, pass1234, etc.
- Change your password regularly or if you believe it may have been compromised.
- If you believe your password may have been used by someone other than you – report it.

Other measures to protect electronic information systems will involve antivirus spyware and firewall to prevent external access to the system. Ensure the backup of your systems are done regularly to prevent loss of information should the system be corrupted or damaged.

Document security.

Personal data held on hard copy documents should be protected from abuse or loss. Your employer will have both policies and procedures to manage the storage, control and archiving of documentation holding personal data. In essence the policy for the safety of hard copy documents has already been stated, only authorised persons to have access to such data. In addition, hard copy documents should be locked in a secure cabinet access to which is controlled by an authorised person. Documents when not in use should be returned to the secure cabinet. Documents should be held in situ and not removed from the home or unit. Maintain a clear desk, that is when away from the desk do not leave personal documents on the desk for others to view.

If you found this information sheet useful why not visit our resource library, where you can find many more items that will help you in your caring role

Please get in touch and let us know what you think of our training and supporting material

Please click on the icons below for full course lists in each of our delivery styles

For more information relating to any of your staff training needs, contact us today

01823 332200 **info@redcrier.com** **www.redcrier.com**