BLSupdate.com

- Information & Governance including Cyber Security -

Understanding Cybersecurity and Information Governance

Information & Governance role

Information Governance is crucial because the law only permits sharing patients' personal data with those who provide care and services to them. However, it's also essential to use this data for secondary purposes such as improving the quality of care, researching treatments, commissioning clinical services, and planning public health services. Personal data should not be shared for these purposes without the patient's informed consent. Personal data is any information that can identify an individual from the data, or other information in the possession of the data controller.

Organisations must safely exchange sensitive health and social care info. Information Governance (IG) is the legal framework that governs its use, transfer, and storage. This module teaches the roles of the Information Commissioner's Office, GDPR principles, and the responsibilities of Data Controllers and Processors. Learners will also study breach prevention and implications.

NHS Healthcare

Information Governance (IG) is a legal framework that regulates the use, transfer, and storage of personal confidential data in healthcare. This framework is governed by several Acts and Regulations, including the 'NHS Act 2006', 'Health and Social Care Act 2012', GDPR, and 'Human Rights Act 1998'. IG provides consistent guidelines for employees handling information, including the various rules and codes of practice such as the 'Data Protection Act', 'Common law duty of Confidentiality', 'ISO/IEC 27002:2005', and 'Freedom of Information Act 2000'. The Code of Practice for the Management of Confidential Information was planned for publication in 2013.

The NHS is dedicated to providing top-notch confidential services, and this is done by processing patient information lawfully, transparently, and fairly. The public has the right to comprehend why their information is processed and give consent for its use and disclosure.

Governing bodies like the GMC and NMC set the confidentiality standards for healthcare professionals. The 'Clinical and operational information governance' enhances the quality of care of patients, governs patient safety, population health, operational efficiency and effectiveness while reducing costs and risk.

The healthcare industry faces various challenges, including:

- The growing use of electronic systems and applications
- A surge in healthcare data volume and variety
- Increasing uses of healthcare information
- Proliferation of medical devices that generate data needing reliable integration into systems
- The state of interoperability across devices and systems
- The reliability of shared and exchanged information.

These challenges accentuate the importance of information governance, as well as the careful consideration that must be given when adopting them. Good sharing of information is vital, but this must be done while maintaining confidentiality. Healthcare organisations must balance both aspects to provide a seamless and integrated service to their patients.

Information governance is the legal framework that governs the NHS. Its primary purpose is to ensure that data is not unlawfully accessed, used, destroyed, recorded, disclosed, modified, inspected, or disrupted.

To achieve this, the NHS must take several measures, including:

- Analysing and documenting the type of personal data held by the organisation
- Ensuring all procedures and processes protect individual rights
- Identifying lawful basis for data processing and ensuring consent procedures are legal
- Regularly implementing and reviewing procedures for detecting, reporting, and investigating data breaches
- Storing data securely and ensuring clear desk policies are adhered to
- Limiting access to sensitive data on IT systems and granting appropriate permissions
- Assessing risks to individual rights and freedoms in the event of a data breach
- Providing appropriate equipment for paper document waste disposal
- Holding data controllers responsible for data processor breaches, unless evidence shows all reasonable steps were taken to ensure compliance.

The Data Protection Officer (DPO) is responsible for informing and advising on an organisation's data protection obligations, conducting 'Data Protection Impact Assessments' (DPIAS), and serving as a contact point for data subjects and supervisory authorities. An organisation needs a DPO if it meets ***one*** of the following criteria: processing by a public authority or body, regular and systematic monitoring of data subjects on a large scale, or large-scale processing of special categories of personal data/data relating to criminal convictions and offences.

Responsibilities

Healthcare workers have several responsibilities, such as securely storing patient records and notes, accessing patient records with consent and ethical considerations, avoiding suspicious or spam emails and unauthorised software downloads, and sharing patient information appropriately and lawfully. Large healthcare organisations like the NHS have different levels of Information Governance responsibilities and awareness. Relevant information on local policies can be found on the staff intranet or obtained from online.

Understanding the Information Commissioner's Office (ICO)

ICO is a UK public body that ensures organisations respect privacy rights. It deals with both 'General Data Protection Regulations' and 'Privacy and Electronic Communications Regulations', handles complaints, ***and*** issues enforcement notices.

The 'Employment Practices Code' helps employers comply with the 'Data Protection Act' and uphold good practices in the workplace. Employers who ignore the code may be subject to a criminal offense.

Personal data in the workplace includes:

- Monitoring health information
- Employment records
- Recruitment
- Selection
- Agency staff
- Sickness-related absences

All UK organisations collecting, processing, or storing personal information must comply with GDPR. ***Failure to comply*** may result in fines of up to £500,000 in case of a data breach.

GDPR protects personal data handling ***and*** the free movement of such data of EU citizens. The 'Data Protection Act' applies to all data subjects, as well as organisations based/processing data in the UK, covering all personal data from health records.

Sensitive Data

Sensitive data is information that requires special care and protection due to its nature. It includes racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, and criminal convictions. Employers may need to process sensitive data related to a worker's physical or mental health, criminal convictions, and special needs during interviews or selection testing. This data is processed to assess suitability for certain types of employment, facilitate adaptations in the workplace, and monitor equality of opportunity. The 'Data Protection Act 1998' and 'General Data Protection Regulations' provide guidelines for the processing of sensitive data, including fair and lawful processing, purpose limitations, data minimisation, accuracy, storage limitation, and integrity and confidentiality.

GDPR / D.P. Act 1998

Both, ***GDPR*** and '***Data Protection Act 1998'*** guide personal data processing, but with varying scope and principles. ***GDPR*** applies throughout Europe and enforces seven principles, while '***Data Protection Act 1998***' is UK-centric and has eight principles. GDPR imposes high fines for breaches and mandates accountability by data controllers and processors. Organisations must prove compliance with written procedures, documentation, and privacy notices, must report breaches immediately, and uphold individual rights like informed consent, access, rectification, erasure, and data portability.

Protection Acts

The ***'Data Protection Act 2018'*** implements the ***GDPR*** in the UK, and data controllers must follow data protection principles for using personal data. The 'Disclosure of Adoption Information' (Post-Commencement Adoptions) Regulations 2005, the 'Electronic Communications Act 2000', the 'Public Health (Control of Diseases) Act 1984' ***and*** the 'Public Health (Infectious Diseases) Regulations 1988' also provide guidelines and regulations for data protection.

Fair Processing Notice (FPNs)

Fair Processing Notices (FPNs) are required under the GDPR to provide accessible information to customers/individuals about how their personal data will be used, and how they can exercise their rights under the GDPR. In healthcare settings, FPNs should identify the Data Controller, the legal basis for obtaining the data, and any governing bodies. FPNs should also include information on why and how information will be collected, how it will be used, how it will be retained and kept secure, and processes in place to ensure confidentiality.

The 'Access to Medical Records Act 1988' and the 'Freedom of Information Act 2000' provide individuals with the right to access any medical report and health record relating to them. Health-or-social-care providers should seek patient consent before disclosing personal information. If disclosure is not permitted, legal action could be taken against the organisation and the individual responsible for the breach.

In summary, protecting sensitive data is crucial, and laws and regulations provide guidelines and principles for data protection. The 'Fair Processing Notices', 'Access to Medical Records', and 'Freedom of Information Act' provide individuals with the right to access personal information, and gives them the right in which disclosure of confidential information is solely lawful with patient consent, public interest, or legal duty.

Specific Rights, SARs, and The Confidentiality Model

The 'Data Protection Act 2018' provides individuals with certain rights concerning their personal data. These include the right to access personal data, the right to update incorrect data, the right to erase data, the right to object to processing in certain circumstances, and the right to data portability. The 'Census (Confidentiality) Act 1991' makes it illegal to unlawfully disclose personal census information.

The ‘Criminal Appeal Act 1995’ gives the ‘Criminal Cases Review Commission’ powers to demand documents or materials from public bodies related to cases they are investigating.

The ‘Gender Recognition Act 2004’ gives transsexual people the legal right to live in their acquired gender and establishes the ‘Gender Recognition Panel’. Applicants to the ‘Gender Recognition Panel’ need to provide medical evidence to support their application, and a full certificate that provides legal recognition of their acquired gender. Information relating to an application for a ‘Gender Recognition Certificate’ is protected information, and it is an offence to disclose it to any other person unless an exemption applies. Exemptions include consent from the person, if the person cannot be identified, if information is needed for the prevention and investigation of crime, or to comply with a court order.

‘A Subject Access Request’ (SAR) is a request for an individual to see a copy of their personal data held by an organisation. SARs can be made in any format and should be passed immediately to the Data Protection Office. Organisations must respond promptly within 40 calendar days. Failure to comply can result in fines of more than £500,000 under GDPR legislation. The right of access includes being told whether personal data is being processed, given a description of the data and its reasons for processing, given a copy of the information, and details of the data source.

The Confidentiality Model outlines requirements for providing patients with confidential service. Record holders must protect patient information and inform them of its intended use while allowing them to choose whether their information can be disclosed or used in particular ways. The model requires continuous improvement in protecting, informing, and providing choice to patients. NHS workers have a legal obligation to protect all sensitive and personal data they encounter, including patient health information, employee records, occupational health records, and confidential business information.

Caldicott and Candour

When handling confidential information, it is important to uphold a duty of confidence, protect and maintain confidentiality, and be cautious about who you disclose information to on a phone call. Ensure that any request for information is clinically justified and the requester is verified. In case of doubt, speak to your manager or Caldicott Guardian, who is responsible for ensuring confidentiality.

The ‘Duty of Candour’ is a CQC regulation for health and social care providers to promote open and honest communication between staff and service users. Providers must follow the regulation when serious incidents occur during treatment or care. It is a legal obligation within the NHS in case of death, serious injury, or minor injury with prolonged psychological harm. Patients should expect open discussions, a non-defensive approach, engagement in investigations and outcomes, and an apology from the healthcare provider. The apology must be made verbally and then followed by a written apology.

Patients have the right to access their personal records and expect privacy and confidentiality. The NHS commits to ensuring access to health and social care data for safe and effective treatment. Anonymised data collected during treatment can be used to support research and improve care. Staff should share any correspondence sent about the patient's care. Each NHS organisation has a Caldicott Guardian responsible for overseeing the control of medical records.

The seven Caldicott principles of using confidential information are as follows:

- The purpose(s) for using confidential information should be justified
- Confidential information should only be used when absolutely necessary
- The minimum amount of confidential information required should be used
- Access to confidential information should be on a strict need-to-know basis
- Everyone who has access to confidential information must understand his or her responsibilities
- Confidential information must be handled in accordance with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

Information security safeguards confidential information and assets by allowing authorised use of technology. All staff must undergo essential training to understand their responsibilities related to information security and be competent to perform their duties. Documents must be created accessibly to avoid the need for braille transcription or audio files. Accurate documentation in clinical records ensures patients can be discussed with all members of the multi-disciplinary team with the absolute minimum of confusion.

Patient Rights

The Government proposed that new rights and pledges for the NHS Constitution must be extended to cover the whole health and social care system. Patients have the right to access their personal records and expect privacy, confidentiality, and information about how their data is used. Patients can request that their confidential data is not used beyond their care, and the NHS and adult social services must ensure safe and effective access to health and social care data for their care and treatment. Identifiable data will be anonymised whenever possible, but patients have the right to object when identifiable data is necessary. Patients must be informed of research studies in which they may participate, and any correspondence related to their care must be shared with them.

Record Usage

When using records for research purposes, follow local policy and guidelines. Keep discussions about people in your care private and do not leave records where unauthorised staff or members of the public might see them. Do not take or keep photographs that are not clinically relevant. Inform people in your care that their health records may be seen by others involved in their care. Respect the right of people in your care to ask for their information to be withheld from health professionals, unless withholding such information would cause serious harm. Report any access or record keeping problems to someone in authority and keep a record.

When handling confidential information, it's important to obtain explicit consent and limit disclosures, unless required by law or in the public interest. Access to information systems must be kept secure, and healthcare providers should keep up-to-date with relevant legislation and policies. Effective communication and record-keeping are also essential.

Patient Consent

Consent is a key decision-making process that allows patients to choose or refuse medical interventions. Healthcare providers must have adequate knowledge of consent and inform patients about their condition in an accurate, easy-to-understand manner. Consent can be given verbally or in writing and must be voluntary, informed, and made by someone with the capacity to make the decision.

Patients have the right to object to the disclosure of confidential information, but this may affect the care that can be provided. Consent is usually not required for information disclosures needed to provide healthcare. Healthcare providers must obtain consent lawfully and ensure the person has the necessary knowledge and understanding of the care or treatment.

Transportation of Sensitive Data

To comply with regulations, sensitive and confidential data should be transported securely. The transportation and packaging method depend on the means of transfer. Several packaging methods, including Envopak carriers, brown paper envelopes, plastic boxes, and lockable pilot bags, can be used. The chosen method must comply with local NHS procedures and be fit for purpose. Returnable packaging should be labelled with the department's return address, and privacy markings should be used on envelopes or packages with personal or sensitive information.

Three types of confidential information - clinical, personal, and business - require approved transportation and packaging methods for internal transportation of records containing confidential information. Health records being transported internally must be securely tied or secured in approved carriers, boxes, or trolleys to prevent patient details from being visible. Data and records should never be left unattended in insecure areas or vehicles, and transit envelopes should not be used for transportation of confidential information. Privacy markings and return address should be used on approved packaging and wrappings/envelopes.

Types of Breach Reporting:

Cyber Security breach - Any breach that can pose a risk to individual rights and freedoms should be reported to the ICO within 24 hours, and near misses should be documented internally as per organisational policies. Breaches can lead to damage to the organisation's reputation, financial loss, loss of confidentiality, and fines for data controllers and processors. Cybersecurity includes technologies/processes and controls to protect data systems and networks from cyber-attacks. Malicious or criminal attacks, which accounted for 47% of data breaches in 2017, are the biggest threat to information security.

Email Phishing and Malware - Criminals may use email attachments and links to trick people into giving away sensitive information or downloading malicious software (malware). Phishing emails are designed to manipulate individuals into making a mistake. To stay safe, individuals should never give out login details to anyone, double check with the supposed sender if they receive a request for sensitive information, and not open links or attachments in unsolicited emails. Suspicious emails should be reported to the ICT department/provider, and unauthorised software should not be installed.

Tracking and Breaches of Data Security - A formal booking out system should be used to record the transfer of data and records manually or electronically, and to record the collection of data and records by an external third party and safe receipt by the receiving party. Personal data breaches may include unauthorised access, deliberate or accidental action, sending data to the wrong recipient, lost or stolen computing devices, alteration of data without permission, and loss of availability of data.

Risk and clean desk policy

Before sharing data, consider the purpose, risk, and how to share it. Comply with the law and obtain explicit consent before disclosing identifiable patient information. Help patients access their information and ensure it's available on a need-to-know basis. Maintain an understanding of information governance appropriate to your role.

Clean desk policy involves securely packing away personal or work items and paper at the end of the day. The policy improves security and aligns with duties of confidentiality and privacy imposed by professional regulatory bodies.

Final Notes

Cybersecurity and Social Engineering Awareness - 'The National Cyber Security Centre' (NCSC) provides information to protect critical services from cyber-attacks and manage major incidents. It helps improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations. The EU Directive on the 'Security of Network and Information Systems' (NIS) becomes UK law in May 2018, and all organisations deemed 'Operators of Essential Services' must comply from this date.

Social Media Overview and Guidelines - Social media refers to technology that enables sharing of information, ideas, and other expressions through virtual communities and networks, such as Facebook, WhatsApp, Instagram, Twitter, and LinkedIn. It's important to comply with the 'Acceptable Use Policy' when using social media for personal or official purposes. Only use social media sites authorised by the organisation and loaded onto the work device, and limit personal use of social media during working hours, unless the job requires the use of specific social media.

Social engineering is an attack method that tricks people into breaking normal security procedures, and individuals should always be vigilant when using the phone, receiving unsolicited emails, using social media, or walking around their place of work.