NEL Commissioning Support Unit

NHS

Lambeth Patient Participation Group Network

Information Governance (IG) Training

Content

- What is information governance?
- Key developments
- The General Data Protection Regulation (GDPR)
- Data protection by design
- Data protection impact assessments
- Data subject rights
- Transparency and fair processing
- Information and data flow mapping
- The role of the Data Protection Officer
- Consent
- Information security

What is Information Governance?

- The management discipline that exploits an organisation's data whilst associated risks and costs are minimised.
- Information Governance (IG) provides a structure which brings together all the requirements, standards and best practices that apply to handling personal and corporate information in an appropriate, confidential and secure manner.
- IG builds patient and staff confidence in how their personal and confidential data is handled.

NEL

Statutory and Mandatory Assurance

The key standards in IG are derived from:

1. The Data Protection Act 2018
2. The Caldicott Principles
3. The NHS Confidentiality Code of Practice
4. The Freedom of Information Act
5. The NHS Records Management Code of Practice
6. The NHS Information Security Code of Practice
7. Common Law Duty of Confidentiality

NEL

What is Personal Confidential Data (PCD)?

- PCD is personal information about identified or identifiable individuals. PCD must be protected.

- Examples of PCD include: name, D.O.B, address, postcode, and general information about a person e.g. medical records.

- Although the Data Protection Act does not apply to the deceased, under the common law duty of confidentiality, there is an ethical obligation which requires confidentiality obligations to continue to apply after death.

NEL

What is not PCD?

- Anonymised data: where data has been effectively anonymised and there is no patient identifiable data, information can be processed freely.

- Corporate data: this may be commercially confidential (e.g. papers regarding organisational restructure). The important distinction is whether the data may be released under FOI.

NEL

Primary and secondary use of PCD

What is the difference?

- Primary use covers the use of data for direct clinical treatment, within a care setting and by a clinician, or a member of the wider direct care team, involved in the care of the patient.

- Secondary use covers all other service commissioning functions such as audit, invoice payment, research, efficiency, planning, analysis etc.

Data Protection Principles

1. Processed fairly and lawfully and in a transparent manner .
2. Obtained and processed only for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purpose.
4. Accurate and kept up to date.
5. Not kept for longer that is necessary.
6. Processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational security measures in place.
8. Not transferred to a country or territory outside the European Economic Area unless adequate levels of protection are in place.

Caldicott and information sharing

Three Caldicott commissions were set up to investigate how the NHS shared patient information.

- They recommend that each health organisation must appoint a Caldicott Guardian to oversee and make decisions on information sharing.
- They created seven Caldicott Principles to help NHS staff know when and how to share information.
- They introduced data security standards to help the NHS combat cyber risks and crime.

NEL

Caldicott Principles

1. Justify the purpose(s).
2. Don’t use PCD unless it is absolutely necessary.
3. Use the minimum necessary PCD.
4. Access to PCD should be on a strict need to know basis.
5. Everyone should be aware of their responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

NEL

Data security standards

- In June 2016, the National Data Guardian published 10 new Data Security Standards.
- The new standards are summarised under three leadership obligations.

1. People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.
2. Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
3. Technology: ensure technology is secure and up-to-date.

NEL

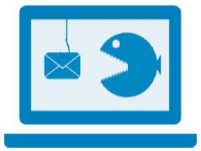
Key developments

Data Protection Officers

Explicit consent and lawfulness of processing

Data portability and access rights

Right to be forgotten

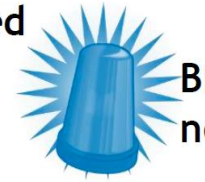


Data protection by design and default

Data transfers and the 'anti-FISA clause'

Freedom of expression and journalism

Measures based on profiling



Breach notifications

Data Protection Impact Assessments

NEL

Headline changes

- Organisations obliged *to demonstrate that they comply with the new law.*
- Requirement to keep a record of data processing activities.
- Tougher fines and penalties for *any* breach of the regulation – not just data breaches.
- Legal requirement for security breach notification - must be reported to the ICO within 72 hours.
- No charge, in most cases, to provide a patient with a copy of their record where they request it (subject access request).

NEL

Headline changes

- Appointment of Data Protection Officer is **mandatory** for all public authorities.
- A data protection impact assessment (DPIA) is required for high risk processing. It is also good practice to complete a DPIA for any major project which requires the processing of personal data.
- There are specific requirements for transparency and fair processing – accessible and in plain language.
- There are tighter rules where consent is the basis for processing. e.g. automated decisions and risk stratification.

NEL

Data protection by design

- Technical and organisational measures to ensure compliance with the data protection principles in both the design and operation of data processing activities is required.
- Measures to include appropriate policies and the use of e.g. pseudonymisation.
- Must ensure that only personal data that is necessary for each specific purpose of processing is processed.

NEL

Data Protection Impact Assessment

Used when planning projects that include PCD.

All NHS organisations must complete a DPIA at project initiation (part of privacy be design).

DPIAs identify privacy risks and address these risks in the final project plan.

- DPIAs are mandatory throughout the NHS.
- Must complete a DPIA for all new services and systems.
- Must also complete a DPIA for changes in services that use PCD.
- Must be completed at the beginning of a project.

NEL

Data Subject's Rights

- Right of access by the data subject
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object
- Automated individual decision-making, including profiling

Right of Access

The Data Protection Act 2018 gives everyone a right to see what information an organisation holds about them and who it has been shared with.

- A request must be in writing.
- It must include adequate identification.
- It must identify what records are requested.
- There is no charge for an individual to access their records.
- An organisation has one calendar month in which to respond [DH best practice says 21 days].
- Exemptions can apply.

Right to Object

- There is a right to object ‘on grounds relating to his or her particular situation’
- Only available where processing is based on
  - ‘legitimate interests’ (not available to public authorities), or
  - ‘task carried out in the public interest or in the exercise of official authority vested in the controller’

Automated Decision Making

- Right to object '…not to be subject to a decision based on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. '
- Doesn't apply where
  - Authorised by UK law which lays down safeguards
  - Explicit consent has been given
- Where e.g. health data processed requires
  - Explicit consent or
  - Substantial public interest and safeguards
- Is likely to apply to risk stratification for case finding
- Applies to the decision not the profiling per se – although note right to object.

NEL

Transparency and Fair Processing

- Information should be '…in a concise, transparent, intelligible, easily accessible form, using clear and plain language, in particular for any information addressed to a child…'
- Specific requirements for fair processing information:
  - The identity and contact details of the data controller or representative.
  - Contact details of the data protection officer.
  - The purposes of processing and the legal basis (Articles 6 and 9).
  - Where 'legitimate interests' applies, what these are (where Article 6(1)(f) applies – not available to public authorities).
  - Recipients or categories of recipients.
  - Any intention to transfer data to a third country or international organisation, with information on adequacy and safeguards.
  - Retention periods or criteria.
  - Existence of rights: access, rectification, erasure, restriction, to object, and data portability.
  - Existence of automated decision-making, logic, significance and consequences for the data subject.

NEL

Data Protection Officer

- Obligatory requirement for public authorities or where processing on a large scale or processing special categories of data.
- Must be independent (although they can be a member of staff or contractor).
- Must report to the highest management level of the organisation.
- Must have 'expert knowledge of data protection law and practices and the ability to perform the tasks specified in the GDPR:
  - Provision of advice to the organisation on compliance obligations, and when a DPIA is required;
  - Monitoring compliance with the GDPR and organisational policies;
  - Co-operating and liaising with the ICO;
  - Taking into account information risk when performing the actions detailed above.

Information Assets and Data Flow Mapping

- Records of processing
- Name of data controller, data processor and contact details of the Data Protection Officer
- Purposes of processing
- Categories of personal data
- Data subjects involved
- Retention
- Technical and organisational security measures
- Processing on behalf of the data controller

NEL

Information asset and data flow mapping

This activity intends to improve the confidentiality integrity (quality), availability of data and records.

- **Information Asset Register**
  Creating an inventory of the records held by each department.
- **Information Asset Owner**
  Identifying individuals who will control and monitor specific assets.
- **Data Flow Mapping**
  Identifying all flows of PCD in and out of the organisation to ensure the method of transfer is secure.
- **Records Management**
  Ensuring the organisation complies with the Records Management Code of Practice in relation to how it creates, stores, retains and destroys its records.

NEL

Consent

- As with the DPA, consent is one condition for processing PCD, with 'explicit consent' a condition for special categories of data.
- As with the DPA, explicit consent is not defined
- As '*consent should not be regarded as freely given if the data subject* ***has no genuine or free choice*** *…'* consent to data processing attached to consent to examination or treatment is unlikely to be valid.
- However, there are other options.

NEL

GDPR, consent and the common law

- ‘Implied consent’ better termed ‘reasonable expectation’ is not valid for GDPR (or now under DPA 2018). However, the GDPR does not invalidate the practice for common law purposes.
- The principle of the Gillick competencies is applicable to children is unaffected, the default age will be reduced to 13 years.
- The GDPR helps here as the exacting requirements for transparency if implemented properly will support legitimate expectation.

NEL

Information Security

It is the practice of applying appropriate controls to safeguard the confidentiality, integrity and availability of information.

- **Confidentiality**: information can only be accessed by authorised individuals on a need to know basis only [access controls].
- **Integrity**: information has not been tampered with, it is reliable and can be used to make informed decision.
- **Availability**: access to information is timely to authorised individuals.

NEL

Information Security – ICO Fine

- The British Pregnancy Advice Service (BPAS) was fined £200,000 when poor records security on a web server resulted in a serious breach of the Data Protection Act revealing thousands of patients' details to a malicious hacker

- BPAS had also breached the Data Protection Act by keeping the patient details for five years longer than was necessary for its purposes

NEL

Information Security Risks

An IG risk occurs when personal confidential data is exposed to unauthorised or inappropriate access, inappropriate processing, theft or loss.

- Lack of IG training and awareness
- Unauthorised access or processing of PCD
- Inadequate records management
- Use of personal and unencrypted equipment
- Untimely IG incident management
- Not having a clear desk
- Emailing incorrect recipient

- Lack of IG training and awareness
- Unauthorised access or processing of PCD
- Inadequate records management
- Use of personal and unencrypted equipment
- Untimely IG incident management
- Not having a clear desk
- Emailing the incorrect recipient

NEL

Information Security - Email

- The previous slide illustrates the most commonly occurring breaches. However, the biggest impact can arise from the smallest breach.
- Malicious emails have become very sophisticated and sometimes highly targeted.
- If you do not recognise the sender (person and organisation) of an email, or it looks suspicious, attempt to verify the sender through a web search or via a telephone call.
- If you think an email is suspicious, delete the email.

NEL

Information Security - Email

- Always be cautious of emails with attachments and/or hyperlinks. Do not open attachments or follow links within unsolicited emails, even if the email appears to be from someone you know or someone within your organisation.

- If you are unsure, verify the sender through a web check or telephone call.

NEL

Information Security – Email

If you suspect your email has been hacked…

- Change your password
- Let your email contacts know
- Change your security question
- Commit to multi factor authentication
- Check your email settings
- Scan your computer for malware and viruses
- Change any other accounts with the same password
- Consider creating a new email address

NEL


Questions