# NHS Lothian local Caldicott, Information Governance and IT Approvals Process

Author: Pavlina Y. McGovern

26 August 2022

# Data Protection

Data protection is concerned with the safe use of personal data. The UK Data Protection Act 2018, which incorporates the EU General Data Protection Regulations (GDPR) outlines the data protection principles that organisations, businesses and the government must follow when using personal data.

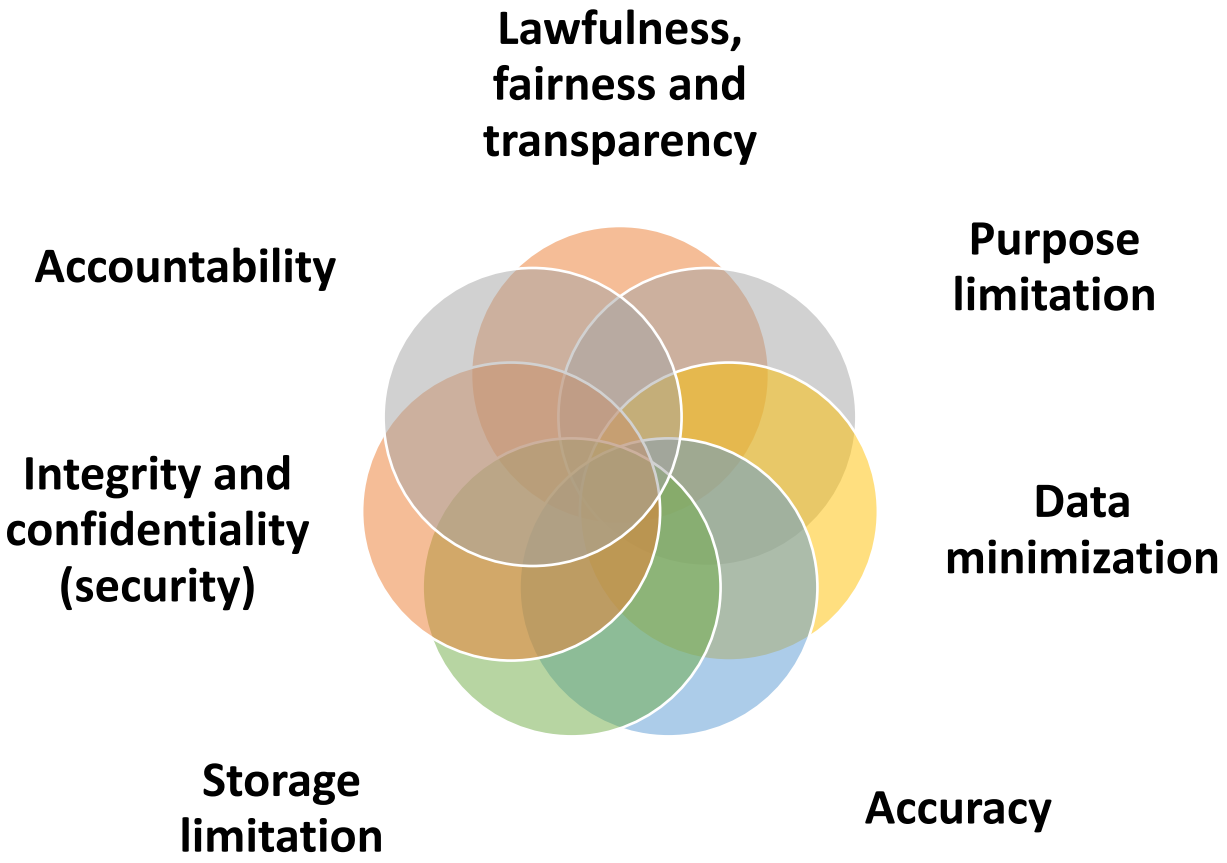
**Personal data**: any information which either alone, or combined with any other data leads to the identification of individual(s). This could be a name or phone number, IP address or cookie identifier.

**Pseudonymous data**: data that have been altered so that no direct identification of any individual can occur. However, additional information is held by you or someone else that allows the identification of an individual. This is personal data and is subject to the Data Protection Act 2018.

**Special category personal data**: data which are subject to more scrutiny when determining the lawful processing. They include things like race, ethnicity, medical conditions (physical and mental), sexual life, religion, philosophical beliefs, politics and trade union memberships, criminal convictions/alleged offences, genetic and biometric data. (from the Information Commissioner's Office website)

**Anonymous data** are not able to identify any individual in the data. Removal of identifiers does not necessarily make the data anonymous. In anonymous data, no combination of variables would allow an individual to be directly or indirectly identified. Anonymous data is irreversible. It is not subject to the Data Protection Act 2018.

# General Data Protection Regulation (GDPR) Principles:



# Data Controllers and Data Processors

Data Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes. Controllers shoulder the highest level of compliance responsibility – you must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements. You are also responsible for the compliance of your processor(s).

Data Processors act on behalf of, and only on the instructions of, the relevant controller. Processors do not have the same obligations as controllers under the GDPR and do not have to pay a data protection fee. However, if you are a processor, you do have a number of direct obligations of your own under the GDPR.

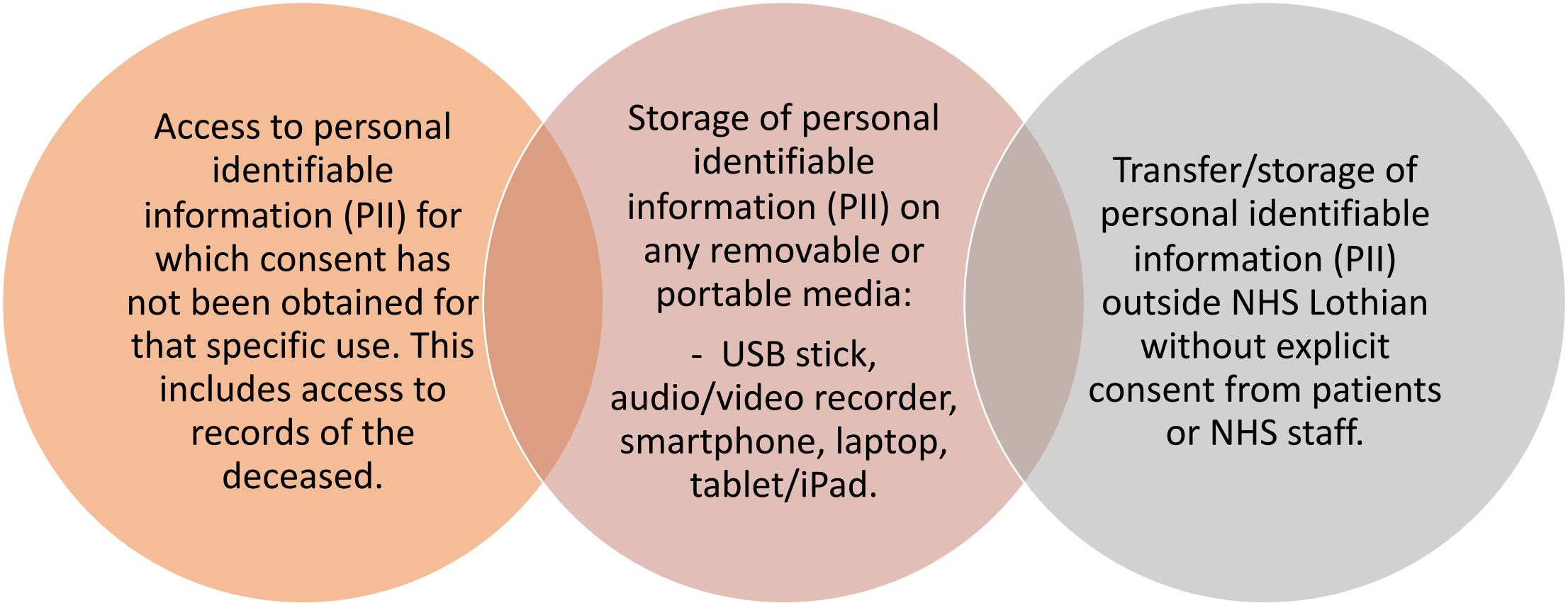
# Local Caldicott – NHS Lothian

The interim Caldicott Guardian for NHS Lothian is Miss Tracey Gillies, Executive Medical Director. In this capacity, Miss Tracey Gillies has delegated authority to designated individuals within NHS Lothian R&D to review and approve, where appropriate, Caldicott applications relating to research activity.

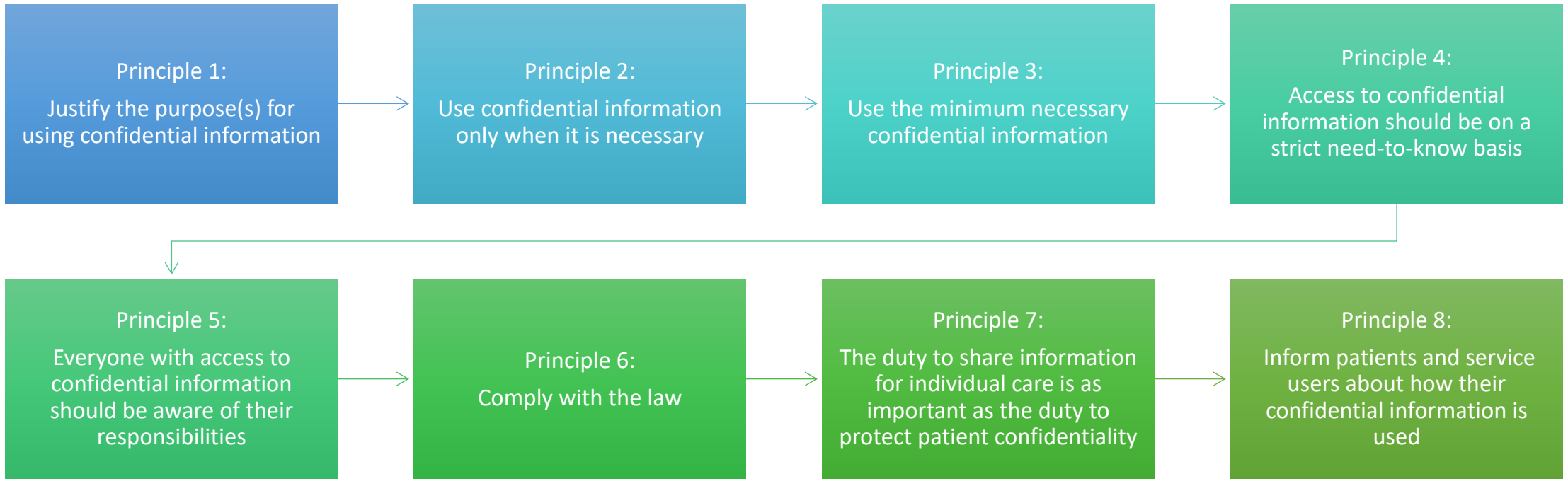
- For any research studies (single centre) requiring local Caldicott Guardian Approval please submit your application to accord@nhslothian.scot.nhs.uk

- For any non-research projects (e.g. service evaluation and audit) requiring Caldicott Guardian Approval please submit your application to caldicott.guardian@nhslothian.scot.nhs.uk

# When is Caldicott approval required?



# The Caldicott Principles




Guidance: [The Caldicott Principles - GOV.UK (www.gov.uk)]

# Consent and Legal basis for processing personal data

Consent is an important part of the research process and is frequently sought for participation in research studies. This is to ensure that any disclosure of confidential information meets the requirements of the common law duty of confidentiality.

Consent to participation in research is not the same as consent as the legal basis for processing under data protection legislation. An example is that a person is asked to consent to participate in research but is told that, if they agree to participate, data about them will be processed for a task in the public interest. The legal basis for data processing is not consent.

# Lawful Basis for Health Research under DPA

## ❑ Processing personal data, under Article 6(1) of GDPR

- *(name, identification number, location data, online identifier, address, age, date of birth, and others)*

* includes pseudonymised data

- Public authorities (NHS organisations, Universities and Research Council institutes)
- 6(1)(e)** task in the public interest

- Commercial companies and charitable research organisations
- legitimate interests

- Use of 'privacy notice' to inform data subjects about processing

- Consent (ensures that the requirements of the common law of confidentiality is met)

## ❑ Processing special category data, under Article 9(2) of GDPR

*(race, ethnic origin, religious beliefs, trade union membership, genetic and biometric data, health data, sex, and sexual orientation)*

- 9(2)(j)** necessary for archiving purposes, scientific or historical research purposes or statistical purposes,
- subject to appropriate safeguards
- in the public interest (proportionate)

- Safeguards:
- controllers must document reasons for any decision that processing is 'in the public interest'
- assessed independently of the Controller

e.g. Peer review from a public funder, REC review, Confidentiality Advisory Group (CAG) for England and Wales, Public Benefit and Privacy Panel (PBPP) for Scotland. Relevant evidence of appropriate review may also be provided by a Data Protection Impact Assessment.

# National Caldicott – Multicentre studies

- If the study involves more than one sites in Scotland, and the collection, transfer and storage of personal identifiable information is not consented, you will need to apply to the Public Benefit and Privacy Panel for Health and Social Care (PBPP): https://www.informationgovernance.scot.nhs.uk/pbpphsc/

  *If carrying out research involving two sites in different Health Boards in Scotland, it is possible to submit local Caldicott application to each of the health boards (e.g. NHS Lothian and Forth Valley).

- If there are sites in England and Wales, you will need to apply to the Confidentiality Advisory Group (CAG).

- If there are sites in Northern Ireland, you will need to apply to the Privacy Advisory Committee (PAC).

# When is PBPP application required?

- **An application to PBPP is mandatory for:**

✓ Any use of sensitive or identifiable NHS Scotland data other than for direct care
✓ Use and linkage of NHS Scotland National Services Scotland ‘national’ datasets
✓ Use of NHS Scotland data from multiple boards
✓ Linkage with external (non NHS Scotland) data
✓ Linkage to primary research data
✓ Access to individuals’ clinical data without consent
✓ For transfer of NHS data out with Scotland

- **An application is optional for:**

✓ Any other use of NHSS data considered sensitive, novel or complex, or with wider national implications
✓ Use of data from primary care providers, and/or from beyond NHS, but with implications for the service

# NHS Lothian Information Governance & IT Security

- **Policy**: In accordance with Scottish Government guidance and the NHS Lothian Digital and IT Security policy, NHS Lothian is responsible for ensuring that all IT assets and personal identifiable data under its control is managed with due care and diligence.

- **Systems Checks**: Any Non-NHS system or software used to store personal identifiable information (PII) needs to be risk assessed by NHS Lothian IG/IT Security
- **Outcomes**:
  - The completed checklist is then used to inform an IT Security risk assessment, identifying levels of risk associated with the system/software to be used.
  - Once the risk assessment is complete, NHS Lothian IG/IT Security will approve the system/software for use and/or provide details of the requirements that must be met. The research team and/or Sponsor must provide assurance that these requirements will be met before NHS Lothian R&D Management Approval is issued for a study.

- For more details, please visit: [NHS Lothian Information Governance and IT Security | Accord]

# NHS Lothian Information Governance

## Policies & Guidelines

- Data Protection Policy
- Digital IT Security Policy
- Information Governance Approvals Process for R&D
- Information Governance Policy
- NHS Lothian IT Security Checklist
- Procedure for Re-approving systems used in NHS Lothian
- Safe Email Transmission Guide
- Safe Video Conferencing

- Link: NHS Lothian Information Governance and IT Security | Accord




# Thank you for your time!

Contact: Pavlina.Y. McGovern@nhslothian.scot.nhs.uk