A Brief Guide to Caldicott Standards and Data Protection

Caldicott Review

The Caldicott Committee, chaired by Dame Fiona Caldicott, carried out a review investigating ways that service user information was used within the health service. Following the review, a report was issued identifying standards to improve the quality of and protect service user information, which the health service began to implement in 1998. The Caldicott Committee identified 6 principals that organisations within the NHS should adopt, known as the Caldicott Principals.

Since then further reviews have been carried out (in 2013 and 2020) and there are now 8 principles, that apply to health and social care service user data.

Caldicott Principles

Principle 1: Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information - in some cases, greater engagement will be required.

Caldicott Guardians

The Caldicott Committee recommended that each organisation within the National Health Service appoint a Caldicott Guardian, whose role is to ensure that high standards of information security and confidentially are implemented across the Trust. Reviews carried out by Dame Fiona resulted in Caldicott Guardians being appointed in all organisations responsible for health and social The Caldicott Guardian represents relevant confidentiality issues to the Board. To reflect the information governance information revolution Dame Fiona was commissioned to review the report, the full findings are available from March 2013.

Data Protection:

In accordance with Data Protection legislation Personal data must be obtained fairly and lawfully. The data subject should be informed of who the data controller is (the organisation); who the data controller's representative is; the purpose or purposes for which the data are intended to be processed; and to whom the data will be disclosed. Personal data processing may only take place if specific conditions have been met- these include the subject having given consent or the processing being necessary for the Data Controller to perform a public task. Additional conditions must be satisfied for the processing of sensitive personal data,

that relating to ethnicity, political opinion, religion, trade union membership, health, sexuality, or criminal record of the data subject

The legislation covers personal data in both electronic form and manual form (e.g. paper files, card indices) if the data are held in a relevant, structured filing system

Personal data processing must be in accordance with the purposes notified by the Trust to the data protection commissioner and documented in the privacy policy on the Trust website- if any 'new processing' is to take place the Data Protection Officer must be consulted

Personal data must be kept accurate and up to date and shall not be kept for longer than is necessary

Appropriate security measures must be taken against unlawful or unauthorised processing of personal data and against accidental loss of, or damage to, personal data. These include both technical measures, e.g. data encryption and the regular backing-up of data files and organisational measures, e.g. staff data protection training

Personal data shall not be transferred to a country outside the European Economic Area unless specific exemptions apply (e.g. if the data subject has given consent) this includes the publication of personal data on the internet

Relevant Policies available on Intranet:

- Information Governance
- Confidentiality Code of Practice
- Records Management
- Data Protection
- Information Sharing
- E-mail Policy
- Intranet Policy
- Information Risk Management

Trust Contacts:

Dr Mehdi Veisi
Caldicott Guardian (CG)
mehdi.veisi@nhs.net

Dr John Heffernan
Deputy Caldicott Guardian
John.heffernan@nhs.net

Sarah Wilkins
Senior Information Risk Owner (SIRO)
sarah.wilkins1@nhs.net

Mark Gregson
Deputy Senior Information Risk Owner
Mark.gregson@nhs.net

Mary Olubi
Information Governance Manager & Data Protection Officer
mary.olubi@nhs.net

Reviewed 20/09/2021