

|  |
| --- |
| Information Governance & Cyber Assurance |
| **Caldicott Approval Protocol** |

|  |  |
| --- | --- |
| **Protocol Manager: Head of Information Governance & Cyber Assurance** | **Policy Group:**  **N/A** |

|  |  |  |
| --- | --- | --- |
| **Policy Established:**  **N/A** | **Policy Review Period/Expiry: October 2023** | **Last Updated: October 2021** |

**This policy does apply to Medical/Dental Staff employed by NHS Tayside**

## UNCONTROLLED WHEN PRINTED

## Role of the Caldicott Guardian

Caldicott Guardians will be responsible for agreeing and reviewing internal protocols governing the protection and use of patient-identifiable information by the staff of their organisation or those shared with other NHSS organisations. Guardians will need to be satisfied that these protocols address the requirements of national guidance/policy and law and that their operation is monitored.

Caldicott Guardians will also be responsible for agreeing and reviewing protocols governing the disclosure of patient information across organisational boundaries, e.g. with social work services and other partner organisations contributing to the local provision of care. These protocols should underpin and facilitate the development of cross boundary working, health improvement programmes and other changes.

## Patient Identifiable Information

The term patient identifiable information means any data item or combination of data items by which a patient's identity may be established. Commonly used patient identifiable data items are;

Forename Surname Address Postcode Telephone No.

Community Health Index (CHI) Number Date of Birth Diagnosis e-mail address

## The Caldicott Principles Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

**Don’t use patient-identifiable information unless it is absolutely necessary.**

Patient-identifiable information items should not be used unless there is no alternative. **Use the minimum necessary patient-identifiable information.**

Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

## 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 they should only have access to the information items that they need to see.

## Everyone 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 aware of their responsibilities and obligations to respect patient confidentiality.

## Understand and comply with the law

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

## The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

## Access Control

Access control is essential for ensuring that only authorised persons have:

* physical access to computer hardware and equipment;
* access to computer system utilities capable of over-riding system and application controls;
* access to manual files containing confidential information about individuals;
* access to computer files and databases containing confidential information about individuals

## Access to Confidential Information about Individuals

Access to person identifiable information will be restricted to those staff who have a justifiable need to know in order to effectively carry out their jobs. The Caldicott Principles underpin the approach that NHS Tayside will adopt.

Restricted access levels will be used to further limit the access of authorised persons to the minimum information that they need to carry out a task or function. This is particularly relevant to information held electronically, but the principles apply to all records, e.g. staff who need access to manual files only for filing purposes should not need to access the information already contained within the files.

There are also legal restrictions on who may see certain patient-identifiable information. Only staff whose responsibilities include the treatment and care of individual patients or who are involved more widely with the treatment or prevention of disease, such as those employed by public health departments, should be permitted access to such information.

## Access Levels and Registration

There will be formal and documented user registration for access to all person-identifiable information held in confidence, where multiple users need access. Although this is mainly applicable to electronically held information, the principles extend to manual files.

It is particularly important that it is clear, at any point in time, just who should have access to what information and the purpose of that access, as well as the use the information is to be put to.

## Applying for Caldicott Guardian Approval to Access or Record Patient Information

**If you intend to access or rely on existing patient identifiable information in any way associated with your study or proposal then you must apply for Caldicott Approval.**

The application process relies upon the completion of an Application Form and Data Processing Specification (appendix 1)

An approved application is relevant to the named research/study/project/audit that is specified in the application. The information provided on that basis must not be used for other purposes.

## The Caldicott Approval Application

The Caldicott Application Form and included Data Processing Specification are in Microsoft Word format. The required information can be typed directly in to the form. The form should be downloaded and saved prior to entry of data, it is not an online form and anything entered whilst viewing will not be automatically saved.

Once the application is completed, the front page should be manually signed by the sponsor and main data user, then the whole document scanned and emailed to:

TAY.informationgovernance@nhs.scot

or sent by post to:

Caldicott, Information Governance & Cyber Assurance Team, Maryfield House South, 30 Mains Loan, Dundee DD4 7BT

The requirements of the application are described below. The application is an approval document and it is expected to contain sufficient information to allow decisions to be made on authorisation. In support of an application, additional information may be provided in support of the application in the form of:

* An Ethics Committee letter of approval, including any recommendations made by the Committee (where ethics approval has not been necessary an indication of that to be included).
* An outline of the research/study/project/audit programme indicating;
  + The purpose of the research/study/project/audit - to conform to Data Protection and Caldicott Principles.
  + Any person identifiable information to be used and any anonymisation that will be applied.
  + The arrangements to be employed in contacting/inviting/informing/interviewing/follow up of individuals as part of the research/study/project/audit, and where this will occur.
  + The management arrangements - to define responsibilities and to ensure that all agreed arrangements take place.
  + Specification of the users and departments/agencies/organisations/companies that will have access to the information - to define responsibilities and if necessary confirm that all have been made aware and will abide by NHS Tayside rules of confidentiality and security.
  + A specification of any manual or computer databases to be devised as part of the research/study/project/audit indicating;
    - Software to be used
    - Who will be developing the database, and their employer
    - Where the database will be run from
    - Relevant security arrangements: access control, backup and restore, ongoing support, etc.
    - The arrangements for disposal of the information held.

Your arrangements for accessing and processing identifiable personal data must be summarised in a separate Data Processing Specification **for each data source**.

## [The Caldicott Application Form](http://eds.tayside.scot.nhs.uk/NHSTaysideDocs/groups/informationgovernance/documents/documents/prod_358056.docx) including [Data Processing Specification](http://eds.tayside.scot.nhs.uk/NHSTaysideDocs/groups/informationgovernance/documents/documents/prod_360808.docx) documents can be accessed on the [Caldicott section of the Information Governance Staffnet page](http://staffnet.tayside.scot.nhs.uk/OurWebsites/InformationGovernance/CaldicottandConfidentiality/index.htm)s

## or by contacting the team at [TAY.informationgovernance@nhs.scot](mailto:TAY.informationgovernance@nhs.scot)

**Definitions**

**Proposal Title:** the name that you will use to identify your study or proposal

**Sponsor Details:** the details of the NHS Tayside person who is supporting the provision of the information in question, usually to be signed by a consultant or service lead in the specialty or service from which the data is to be sourced/accessed.

**Data User Details:** the details of the person who is mainly responsible for the work to be undertaken using the data to be provided.

**Name and Data Protection Reg. No:** only required for non-NHS Tayside organisations or agencies.

**Data Co-users:** a list of individuals who will have access to the information provided and who will be under the management/supervision of the Data User.

**What Information do you require and what is the intended use:** in straightforward language, and in sufficient detail to understand the proposal, a brief description of the proposal including aims, objectives and methods. In particular, it should be clear whether the proposal relates to audit and service improvement or research.

**Consent:** describe at what stage any required consent is to be sought from the people whose personal data you wish to access, or where there are barriers to gaining consent, please describe those barriers.

**Caldicott Principle 1 – Justify the Purpose(s):** every proposed use or transfer of patient- identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

**Caldicott Principle 2 – Why is Patient Identifiable Information required? :** Patient identifiable information items should not be used unless there is no alternative.

**Caldicott Principle 4 – Is access to the data on a need-to-know basis? :** Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

**Caldicott Principle 5 – How will you ensure that everyone with access to the data is aware of their data protection and confidentiality responsibilities? :** Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect patient confidentiality.

**Caldicott Principle 6 – How will your organisation’s legal requirements for the use of the data be met? :** Every use of patient-identifiable information must be lawful. Someone in each Organisation should be responsible for ensuring that the organisation complies with legal requirements.

## Data Processing Specification

Unless patient identifiers are required to meet the purpose of the request, only anonymised or pseudo-anonymised data should be requested (in pseudonymised data, identifiers are replaced by an index number)

As patients may be identified from a combination of variables in anonymous data, such as date of birth, date of admission, treating hospital, area of residence, please request only the minimum data required to meet the purpose of the study.

**Caldicott Principle 3 – Why is each data item required? :** where the use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification and the possibility of a breach of confidentiality.

**Data Transfer:** give details of how the requested information will be transferred to you from the Data Source e.g. encrypted USB device, password protected file, paper, NHSmail attachment, etc.

**Safeguards :** describe the measures in place to protect and manage the data securely and confidentially.

**Data Transfer Regularity:** how often do you intend the requested data to be provided to you?

**Data Retention:** how long do you intend to retain the information that you will rely on for your study and how will you dispose of the information at that time?

**Submitting the Caldicott Application**

Once the Caldicott application has been completed and all supporting documentation gathered then the application should be submitted to:

|  |  |
| --- | --- |
| By Mail | **By email** |
| Information Governance & Cyber AssuranceMaryfield House (South)Mains LoanDundeeDD4 7BT | [TAY.informationgovernance@nhs.scot](mailto:TAY.informationgovernance@nhs.scot)  Subject line to be: Caldicott Application: *Topic* |

## Confirmation of Approval

Once Caldicott authorisation has been granted the Data User will receive a letter of approval (Sponsor and any Additional Data Users copied into the approval letter).