Heartbeat
Connecting health and care communities

Caldicott Policy

Version	1
Date	07.01.2022
Approval date	20.04.2018
Approved by	Lisa Pammen
Author	Lynn Irwin
RENEWAL DATE	January 2025

PURPOSE

The principle of Caldicott Guardianship was established in 1997 following the publication of the Caldicott Report from the review chaired by Dame Fiona Caldicott. The review was commissioned by the Chief Medical Officer because of increasing concerns about how patient information was being used in the NHS, specifically the way in which it was being stored and transferred electronically.

The report made 16 recommendations regarding the safeguarding of patient-identifiable information, including the requirement for NHS organisations to appoint a Caldicott Guardian. It also established the original six Caldicott principles, which should be considered before any disclosure of patient identifiable information in order to protect patient confidentiality.

A later review revisited the Caldicott principles, which remained the same except that they no longer refer to "patient identifiable information" but "personal confidential data". More importantly however, the review introduced a new seventh principle.

1. Justify the purpose(s)
2. Only use it when absolutely necessary
3. Use the minimum amount of personal confidential data necessary to perform the task
4. Access to patient-identifiable information should be on a strict "need-to-know" basis
5. Everyone must understand their responsibilities
6. Everyone should understand and comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality.

POLICY/PROCEDURE

THE CALDICOTT GUARDIAN/INFORMATION GOVERNANCE LEAD

For a federation, whilst a Caldicott Guardian is not required, an Information Governance Lead should be appointed (also requirement 114 of the IG Toolkit).

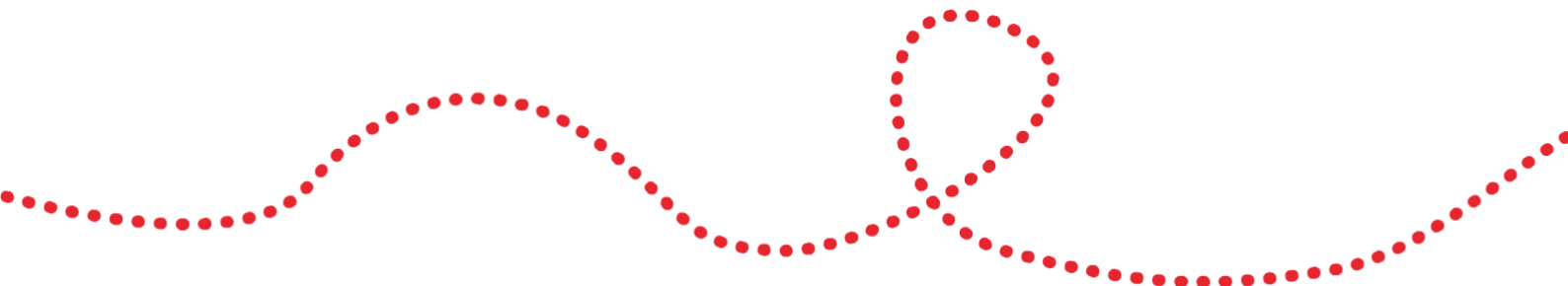
The Information Governance Lead will be a senior member of the staff, generally a clinician, who is responsible for information governance within the practice. Where the lead is not a clinician, this person is expected to have nominated support from a clinical advisor.

RESPONSIBILITIES

Another recommendation within the Caldicott report was that organisations should regularly audit patient information flows and apply the Caldicott principles against each information flow.

This may be achieved by ensuring that information flows are considered as part of the IG Lead's four main areas of responsibility:

1. Strategy and Governance – strategic overview and representation
2. Confidentiality and data protection – knowledge of confidentiality and data protection
3. Internal Information Processing – practice procedure and policy compliance
4. Information Sharing – information provided externally to be assessed, controlled and compliant



The IG Lead should be very familiar with the key influential guidance and legislation, such as the Data Protection Act 1998 and Confidentiality: NHS Code of Practice. He/she should be responsible for operational implementation of information governance in the alliance. For example, making sure there is an IG policy with procedures for staff to follow, ensuring training is made available to staff etc. He/she should also maintain an overall awareness of information flows, internal and external developments and initiatives relating to IG, and ensure that these are measured against ethical and legal standards on behalf of the practice. This may involve assessing and challenging the sharing of information between the practice and other organisations or NHS health bodies.

Where the IG Lead is not a GP, there should be a General Practitioner who takes the lead on tricky data sharing/disclosure issues.

The Caldicott Principles

1. ***Justify purpose***

Every proposed use or transfer of patient-identifiable information within or from the alliance should be clearly defined or scrutinised. Continued use of information should be subject to regular review by the Information Governance Lead.

2. ***Only Use When Necessary***

Where it is not necessary to identify the patient within a flow of information, then this identifying information should be excluded. The need for the identification of a patient should be considered at each stage of a process, and this information should not be provided unless there is no alternative.

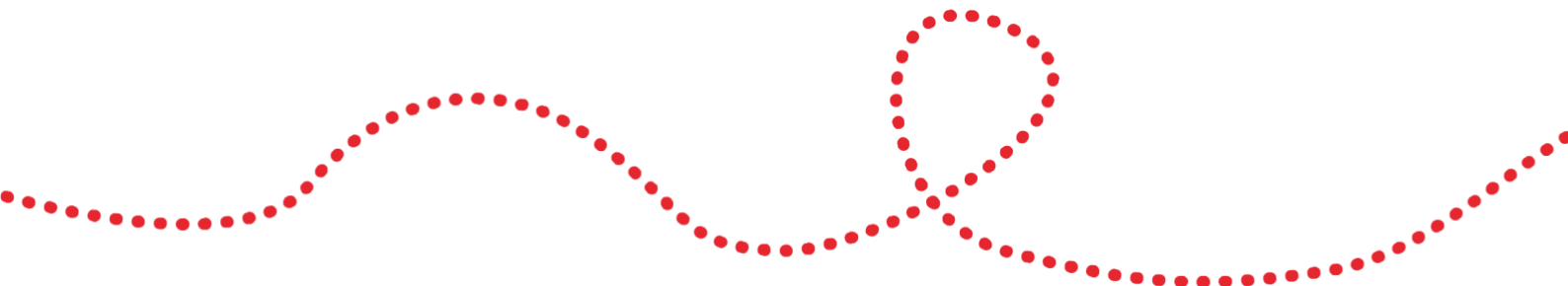
3. ***Use the Minimum Necessary***

Where identifying information is essential, only use the minimum amount to enable the patient to be identified positively, e.g. use of unique patient number combined with date of birth may be sufficient to identify the patient without the possibility of error, negating the need to use names and addresses. Where the use of identifiable information is considered essential, then each individual item of information within the data set should be justified with the aim of reducing identifiability, and therefore the resultant risk should the information be illegally accessed.

4. ***Access on a Need-to-Know Basis***

Only persons who need to have the information should have access, and then only to the parts of the record they need. This may involve access control, the split of access rights, or the split of processes or information flows to ensure that this can be achieved. IG Leads will be responsible for the agreement and the review of internal patient flows and protocols to ensure that patient-identifiable information is protected.

5. ***Awareness of Responsibilities***



All staff should receive training and awareness briefings, with suitable clauses in policy documents and contracts of employment. Both clinical and non-clinical staff should to be aware of the practical application of the requirements in patient-facing situations.

6. ***Comply with the Law***

The IG Lead (and others) within the alliance should maintain a knowledge of relevant legislation (see above) commensurate with their role and level of responsibility. The IG Lead should be responsible for compliance with legal requirements.

7. ***The Duty to Share Information***

Staff should be confident that they can share information when it is in the best interests of patients and within the framework of the Caldicott Principles.

CALDICOTT REVIEW 2

In 2012, Dame Fiona Caldicott was asked to lead a second piece of work - this time because of concerns regarding the balance **- or rather the imbalance -** between the protection of patient information and the use and sharing of information to improve patient care. Basically there was a growing concern that IG was being used as an excuse for not sharing information, even when it would have been in the patient's best interests

The resulting report (Information: to Share or not to Share? The Information Governance Review, March 2013) commonly known as the Caldicott2 report, makes 26 recommendations. The key message from the report is that all organisations providing health and social care services must succeed in maintaining confidentiality and information governance standards, but also practice good sharing of information when this is appropriate.

The report also recommends that regulatory, professional and educational bodies should ensure that sound record keeping **and the importance of data quality,** are part of continuous professional development and assessed as part of the professional revalidation process.

All of the 26 recommendations were accepted by the Government in their response to the review.

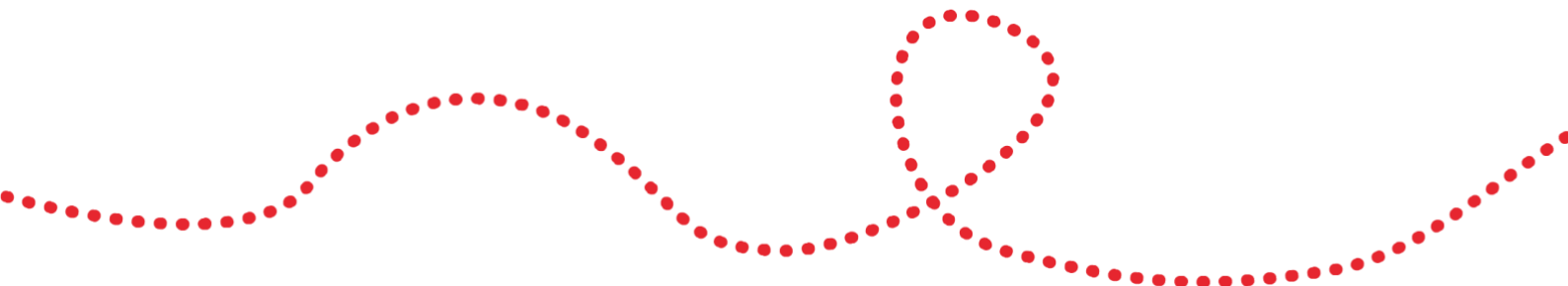
CALDICOTT AUDIT

A tool for auditing the Alliance's compliance with Caldicott is provided as **Appendix A**.

This exercise should be ongoing and repeated on an annual basis.

INFORMATION FLOW MAPPING

See **Appendices B – D**.



PRACTICE STAFF GUIDANCE

Members of staff have a responsibility to ensure security of patient data, which may be held in various forms such as computer-held records, paper files, CCTV images, videos etc. On a day-to-day basis, the Caldicott principles will apply mainly to patient-identifiable data held within paper-based medical records or on a patient-based clinical system.

Basic principles of information handling within the Alliance are:

- Patients should be informed how their data is used
- Patients should be informed who will have access to their data, and when/why
- There should be an understanding of data which may only be released with express consent
- Staff should be aware of patients' rights to access their record, and to discuss / correct errors
- Patients who wish to have their information withheld for a specific purpose should have their rights respected unless there are special circumstances – statutory matters, court orders, public health issues etc.
- Where disclosure is to take place regardless of patient consent, there should be an attempt to agree or discuss the issues with the patient first
- Access to patient information must be strictly on a health-needs basis, and staff should only access patient records when it is required to perform business tasks
- Records must remain secure and confidential at all times. Access to records on computer systems should be password protected, and staff should not leave their terminal whilst still logged on
- Contracts of employment, staff handbooks, visitor agreements, and sub-contractor agreements will contain a specific confidentiality clause

ACCESS CONTROLS

Manual records

- To be held in a lockable area
- Storeroom door kept closed and notes not left in consulting or general office areas
- Filing cabinets locked. Rooms locked outside normal surgery hours
- Reception cover always in place to prevent non-staff access to secure areas
- Records only removed from the practice for specific purposes (e.g. home visits) and returned same day (not held off-site overnight)

Computerised Records

- Differential access rights in force related to role
- Full audit trail facilities
- Access levels controlled by nominated senior staff member or manager
- Automatic password change prompts on all systems
- New starters and leavers to have immediate access status updates
- Active screen savers cut in at short delay intervals
- Privacy filters in use in risk locations (e.g. consulting rooms)
- Consulting room screens cleared of last patient detail prior to calling next patient in
- Automatic log-out of systems when unused for short time period

- Full back-up and storage protocols in place

Sharing of Information

- All external information flows documented and retained securely
- All confidentiality agreements documented and retained securely
- No confidential information passed to third parties without express consent (where appropriate)
- Community staff have access, subject to agreement, commensurate with their role

General

- Visitor log maintained
- Confidential conversations conducted relative to the security of the environment
- Original medical records not released to third parties
- Emailing of patient data restricted to NHS.NET

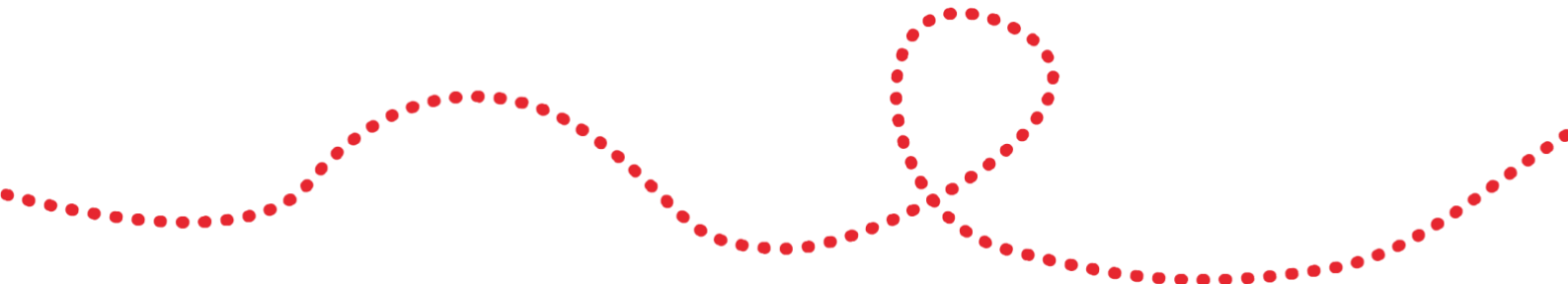
POLICIES / PROTOCOLS

Organisations are recommended to have the following protocols / policies in place to support Caldicott principles.

- Confidentiality of Patient Data [*]
- Access to Medical Records [*]
- CCTV Policy and Code of Practice [*]
- Clinical Governance Policy [*]
- Computer and Data Security Policy [*]
- Computer, Internet and Email Policy [*]
- Confidentiality Policies/Agreements (various) [*]
- Data Protection Policy [*]
- Disclosure / Sharing of Patient Information Policy [*]
- Electronic Transfer of Patient Data policy [*]
- Fax Handling Protocol [*]
- Freedom of Information Act Policy [*]
- Practice Security Procedures [*]
- Risk Management (Toolkit) [*]

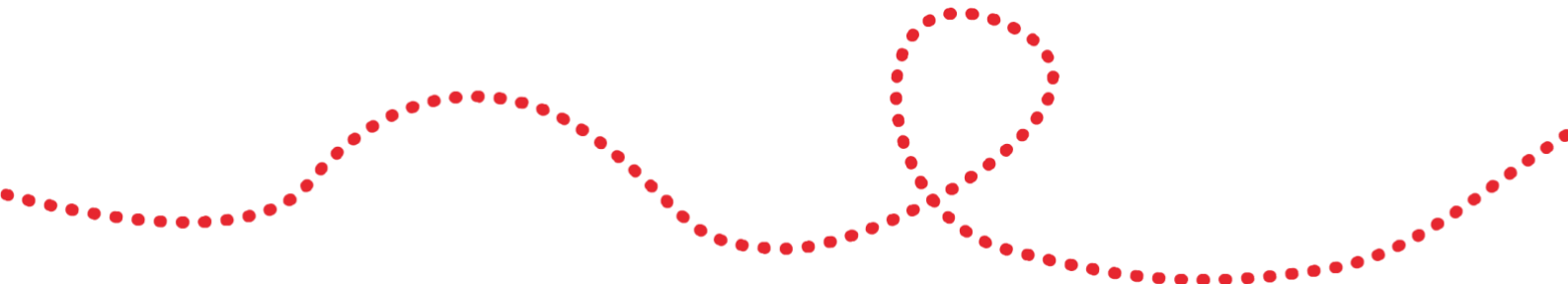
Since the original Caldicott report was published in 1997, a number of other statutory regulations have added to and enhanced the principles of Caldicott. Some examples of these include:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Equality Act 2010



And other guidelines have been published such as:

- NHS Code of Practice on Confidentiality (2003)
- The NHS Constitution for England
- The Care Records Guarantee
- A Guide to Confidentiality in Health and Social Care, HSCIC
- Code of Practice on Confidential Information (draft out for consultation) HSCIC
- The Caldicott Guidance Manual 2010
- IG Toolkit requirements
- Information: to Share or not to Share? The Information Governance Review, April 2013
- Information: to Share or not to Share, Government Response to the Calidcott Review, Sept 2013



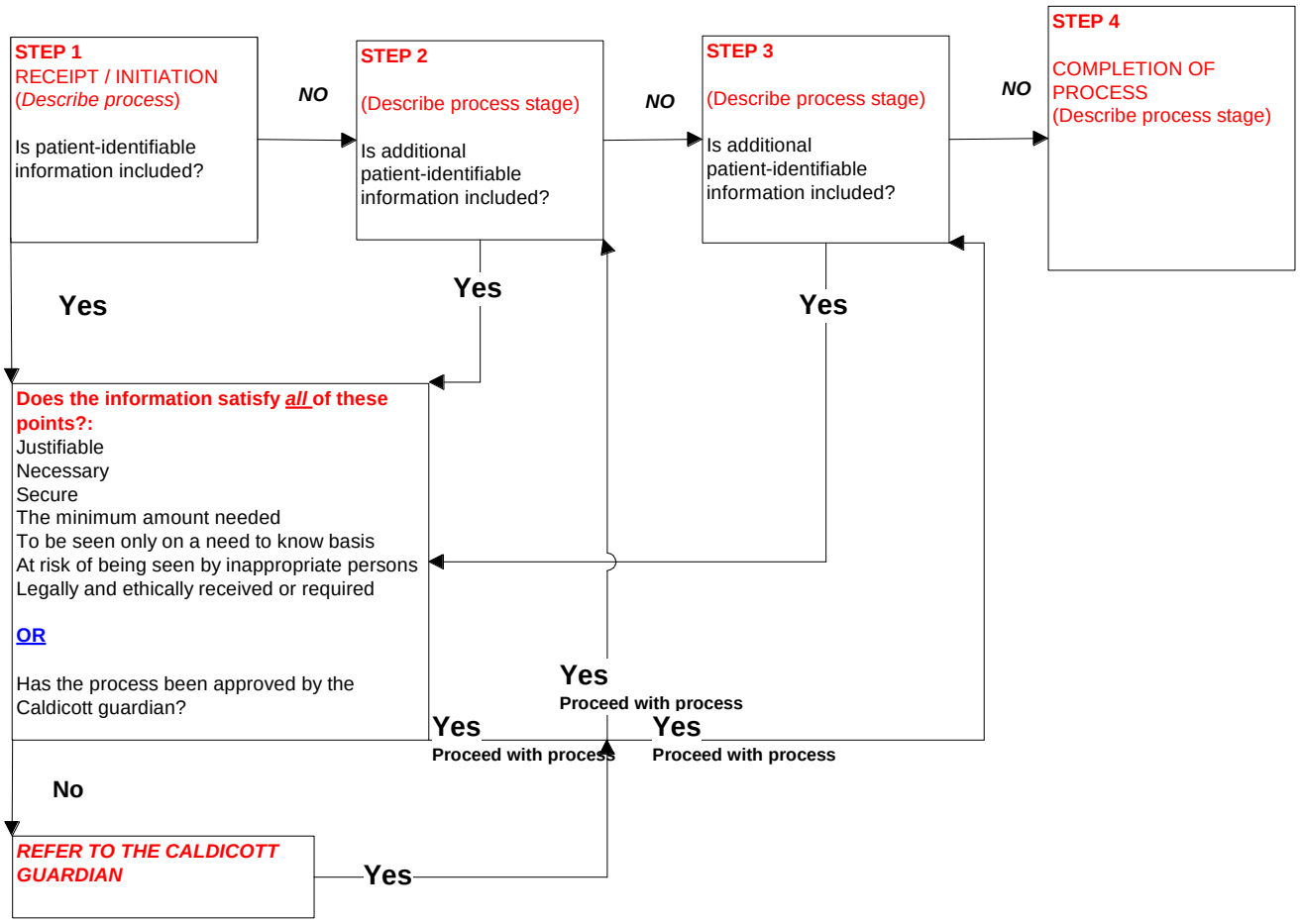
Appendix A - ALLIANCE AUDIT MODEL

ITEM	*Unsatisfactory*	*Acceptable but could be improved*	*Satisfactory*
Information provided to patients on the use of their information	No information provided or limited to simple posters and leaflets in the waiting room	An active information campaign in place to promote understanding of NHS information requirements	An active information campaign supported by comprehensive arrangements for patients with special / different needs
Staff Code of Conduct for Confidentiality	No code exists, or staff not generally aware of it	Code of Conduct exists and staff are aware of it	Code regularly reviewed and updated as required
Staff Induction procedures	No mention of Confidentiality and security requirements in induction for most staff	Basic requirements outlined as part of the induction process	Comprehensive awareness undertaken and comprehension checked
Confidentiality and Security training needs	Training needs not assessed systematically for most staff	Training needs only assessed as a consequence of systems changes	Systematic assessment of staff training needs and evaluation of training that has occurred
Training Provisions (confidentiality and security)	No training available to the majority of staff	Training opportunity broadcast with take-up left to managers discretion	In house training provided for staff
Staff Contracts	No reference to confidentiality requirements in contracts	Confidentiality included in some staff contracts	Confidentiality included in all staff contracts
Contracts with other organisations	No confidentiality requirements included	Basic agreements of undertaking signed by contractors	Formal contractual arrangements exist with all contractors and support organisations
Reviewing information flows containing patient identifiable information	Information flows have not been comprehensively mapped	Information flows have been mapped and management has been informed	Procedures are in place to regularly review information flows and justify purposes
Internal information data	Information flows have not been	Ownership established for all information data sets and register	All owners justify purpose and agree staff access restrictions with the IG

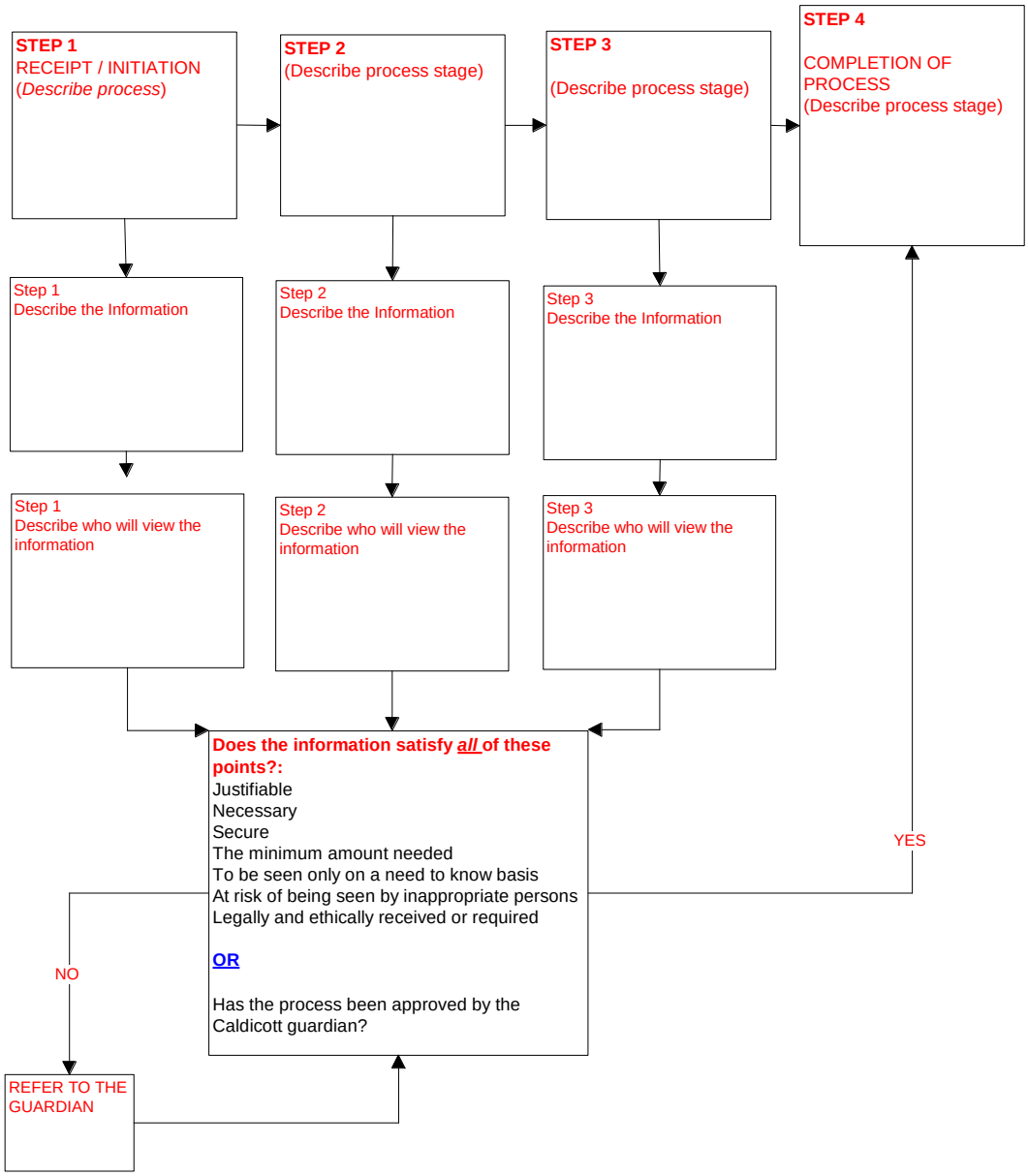
ownership established	comprehensively mapped	established	Lead/Caldicott Guardian
Safe haven procedures in place to safeguard information flows into the Practice	No safe haven procedures in place	Safe haven procedures used for some information flow	Safe haven in place for all patient identifiable information
Protocols for sharing information with other local organisations agreed	No locally agreed protocols in place	Partner organisations clearly identified and information requirements understood	Agreed protocols in place to govern the sharing and use of confidential information
Security policy document	No security policy available	Security policy exists but not reviewed in the last 12 months	Security policy reviewed annually and reissued as appropriate
Security responsibility	No information security officer, or existing officer not fully trained	An appropriately trained information security officer is in place	Responsibility for information security identified in a variety of staff roles and is coordinated by the IG Lead/Caldicott Guardian
Risk Assessment and management	No programme of information risk management exists	A risk management programme is underway and reports are available	A formal programme exists with regular reviews reports and recommendations
Security incidents	No incident control or investigation procedures	The security officer handles incidents as they occur	Procedures are documented and accessible to staff to ensure incidents are investigated promptly
Security monitoring	No monitoring or reporting of security effectiveness or incidents takes place	Basic reporting of major incidents or problems areas only	Regular reports to management on the effectiveness of information security
User responsibilities	No guidance to staff on password management	Users encouraged to change passwords regularly at their discretion	Password changes enforced on a regular basis
Controlling access to confidential patient information	Staff vigilance or "honour" system to control access. Some physical controls	Access for many staff on an "all or nothing" basis. Staff group access agreed with IG Lead/Caldicott	All staff have defined, documented access rights agreed by the IG Lead/Caldicott Guardian. Access

		Guardian	controlled monitored and audited

Appendix B - MODEL INFORMATION FLOW MAP



Appendix C - Information Process Map and Sign-Off Authority



Name of process or project / release of information _____

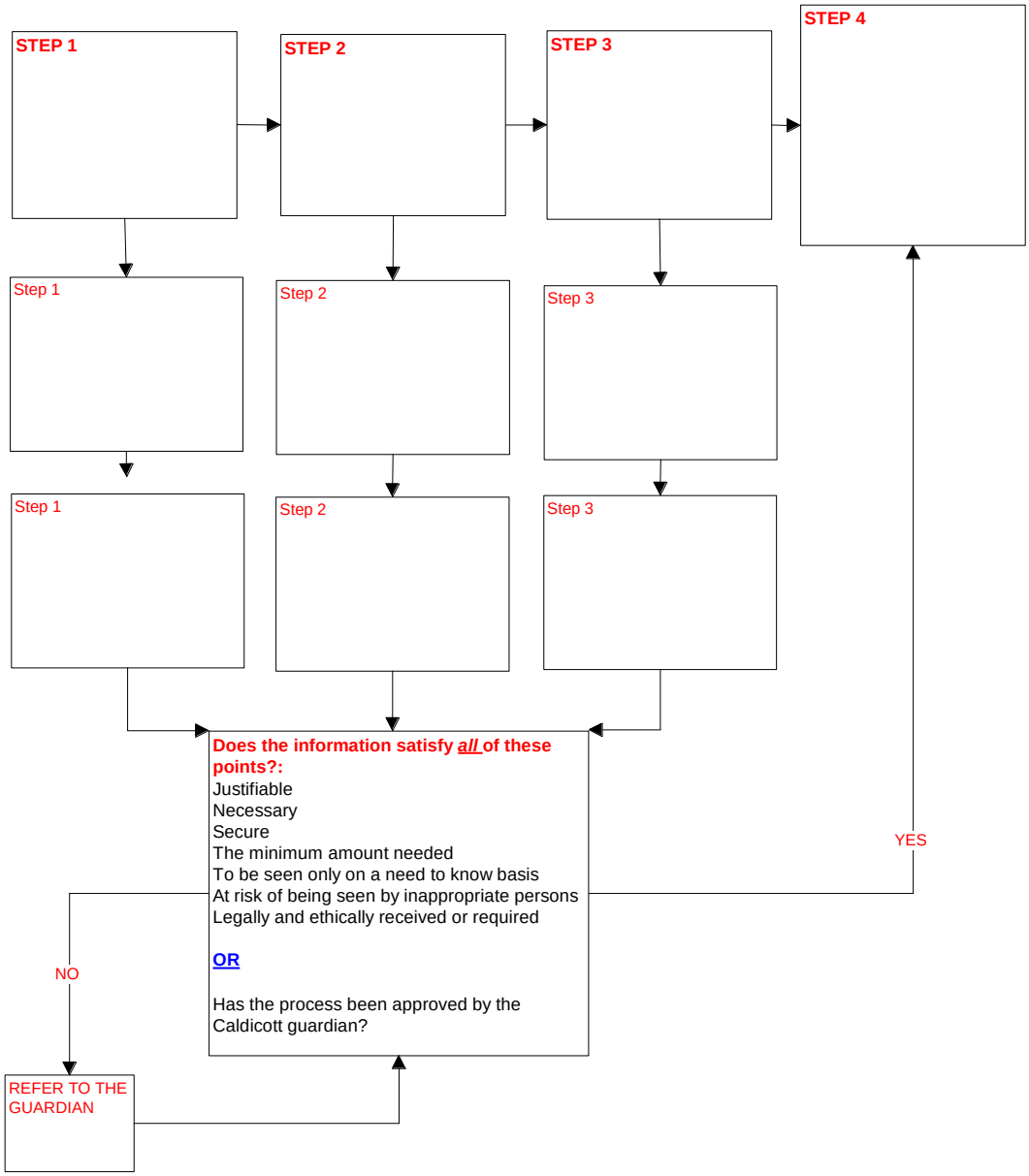
Approved by _____ (IG Lead/Caldicott Guardian) _____ (Date)

Restrictions / Further requirements _____

_____

_____

Appendix D - Blank Template



Name of process or project / release of information _____

Approved by _____ (IG Lead/Caldicott Guardian) _____ (Date)

Restrictions / Further requirements _____

_____

_____

_____

_____