Lister House Surgery

Information Governance, Caldicott and Data Security Policy

Document Details

Classification:	IG
Author and Role:	Cath Anderson
Organisation:	Lister House Surgery
Document Reference:	Information Governance, Caldicott and Data Security Policy
Current Version Number:	7
Current Document Approved By:	Dr Brooks
Date Approved:	March 2020

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of Lister House Surgery.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Lister House Surgery.

If you are updating this document on the shared drive, please do so at C81072\A_Z Policies and Protocols only. It is your responsibility to check for any versions associated with compulsory Blue stream training, the Lister House Website or on You-manage or MS Teams. If updates are required in these areas please inform the Quality Team. Clinical tools bookmarks

B. EQUALITY STATEMENT

Lister House aim to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.
In carrying out their function, Lister House surgery must have due regard to the Public Sector Equality Duty (PSED). This applies to all activities for which Lister House are responsible, including policy development, review and implementation.

C. DUE REGARD

This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination; harassment; victimisation; to advance equality of opportunity; and foster good relations between the protected groups.

If staff or patients wish to raise concerns. Please see-
S:\C81072\Policies and Protocols\ A_Z Policies and Protocols \HR Policies**Whistleblowing Policy**
S:\C81072\Policies and Protocols\ A_Z Policies and Protocols \HR Policies**Grievance Policy**
S:\C81072\Policies and Protocols\ A_Z Policies and Protocols \Quality Policies\Complaints associated documents\ **Complaints policy**

D. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments	Review Due
1	Feb 2007	Cath Anderson	Cath Anderson		
2	April 2010	Rachel Boldison	Andrew Brooks	Combined with Safe Haven and Information Governance Policies.	
3	March 2012	Rachel Boldison	Andrew Brooks	Reviewed and signed off. Added to Induction Folder and Signed understanding by all staff.	April 2014
4	April 2014	Rachel Boldison	Andrew Brooks	Reviewed no changes made	April 2016
5	April 2016	Rachel Boldison	Andrew Brooks	7th Caldicott Principle added to the policy. SIRO Role added and explained. Bluestream added as training provider.	April 2017
6	July 2016	Rachel Boldison	Andrew Brooks	Added Useful Contacts	July 2018
7	March 2018	Carole Plant	Steve Chapman	Amended for Applicability to new sites and governing authority	March 2020
	March 2020	Rachel Boldison	Andrew Brooks	Reviewed updated Appendx B re: training to include GDPR and IG	March 2022

INFORMATION GOVERNANCE / CALDICOTT /SAFE HAVEN PROTOCOL

1. INTRODUCTION AND POLICY STATEMENT

2. INFORMATION GOVERNANCE SCOPE

3. CALDICOTT PRINCIPLES INCLUDING OUR NAMED CALDICOTT GUARDIAN

4. PRACTICE STAFF INFORMATION GOVERNANCE AND CALDICOTT GUIDANCE

5. ACCESS CONTROLS – SAFE HAVEN PRINCIPLES

5.1 GENERAL INFORMATION ON SENDING FAXES

5.2 INCOMING AND OUTGOING MAIL

5.3 TRANSPORTING CONFIDENTIAL AND SENSITIVE DOCUMENTS

5.4 SENDING PATIENT IDENTIFIABLE INFORMATION ELECTRONICALLY

5.5 SHARING OF INFORMATION

5.6 GENERAL GUIDANCE

5.7 FREEDOM OF INFORMATION (PLEASE ALSO REFER TO SPECIFIC POLICY)

5.8 WHO CAN APPLY FOR INFORMATION?

6. RECORDS MANAGEMENT

7. DATA PROTECTION GUIDANCE – 8 BASIC PRINCIPLES

8. NHS CONFIDENTIALITY CODE OF PRACTICE

9. TRAINING AND AWARENESS

10. LEGAL COMPLIANCE

11. PATIENT CONFIDENTIALITY STATEMENT

12. BREACHES OF CONFIDENTIALITY

1. INTRODUCTION

The Practice recognises the vital contribution that reliable information makes to the clinical management of individual patients and the efficient management of services and resources. We also understand that there is an appropriate balance between openness and confidentiality in the management and use of data and records. This policy sets out the framework for ensuring that information is used effectively, efficiently, securely and legally.

All NHS employees are responsible for maintaining the confidentiality of personal and sensitive information. Information will be defined, and, where appropriate, kept confidential; underpinned by the Caldicott Principles and the the requirements of the Data Protection Act.

Treat it like your own – it is a requirement by Statute and Common Law

Policy statement

It is the policy of the Practice to comply with the various applicable Information Governance obligations, including:

- The law;
- Protocols, guidelines, standards etc issued by NHS Southern Derbyshire CCG, the Department of Health (DoH), professional bodies and other relevant agencies;
- Agreements reached with partner organisations.

2. INFORMATION GOVERNANCE SCOPE

This policy covers the use and management of information in all formats including the collection, processing, storage, communication and disposal of information, including (but not limited to):

Patient/Client/Service User Information

Personnel Information (includes all aspects of personnel/HR information)
Organisational Information (including corporate records, financial, contractual and activity data)
Information held on behalf of other organisations
Structured and unstructured record systems – paper and electronic (including archived material)
Transmission or transfer of information – fax, e-mail, magnetic or optical storage media, post and telephone

The policy applies to all employees, temporary staff and contractors working for, or supplying services for the Practice. With relation to non-computer related aspects of information governance, independent contractors may chose to adopt the whole policy or develop their own variation of it.

Any breaches of this policy will be investigated and could lead to disciplinary or legal action being taken against those found responsible.

3. CALDICOTT PRINCIPLES

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 basis of the review by the Committee was to safeguard patient-identifiable information and ensure that the use and the sharing of this information between various bodies was both justified and also limited to essential information only. A 7th Caldicott Principle was added in March 2013 review by Dame Fiona Caldicott.

Since 1997 a number of other statutory regulations have added to and enhanced the principles of Caldicott, and some of these are:

- Human Rights Act 1998
- Data Protection Act 1998(Principle 7): 'Appropriate technical and organisational measures shall be taken to make personal data secure'.
- Freedom of Information Act 2000

Other guidelines have been published such as:

- NHS Code of Practice on Confidentiality (2003) Annex A1 Protect Patient Information *'Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are as secure as they can be'.*
- NHS Care Records Service, and the IT Directed Enhanced Service provisions especially those relating to staff training and data quality
- The Cayton Review of NHS Information Governance (2006)
- Computer Misuse Act "You must ensure that you only access the systems, databases or networks to which you have been specifically authorised to do so. You must also report any suspected attempts or unauthorised access by others."

THE CALDICOTT GUARDIAN

OUR IG LEAD and CALDICOTT GUARDIAN IS DR BROOKS
supported by Rachel Boldison

RESPONSIBILITIES

One of the original recommendations to the Caldicott report was the regular auditing of patient information flows within the Practice or organisation. This was defined within 7 principles:

And these may be applied by ensuring that they are considered as part of the Guardian's 4 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 Guardian should maintain an overall awareness of information flows, internal and external developments and initiatives, and ensure that these are measured against ethical and legal standards on behalf of the Practice. This may involve assessing and challenging the provision of information between the Practice and other organisations or NHS health bodies, including the CCG.

THE 7 CALDICOTT PRINCIPLES (See Flowchart at Appendix E)

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. 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. They should be supported by the policies of their employers, regulators and professional bodies.

4. PRACTICE STAFF INFORMATION GOVERNANCE AND CALDICOTT GUIDANCE

The Business Practice Manager is the Senior Information Risk Owner for the Practice. His role is to lead and foster a culture that values, protects and uses information for the success of the organisation and benefit of its customers / patients.

- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently.

- To take visible steps to support and participate in that plan (including completing own training)

- Informing the Caldicott Guardian/IG Lead of information risks

All 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 Practice 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 required to do so to perform their 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 or employment, staff handbooks, visitor agreements, and sub-contractor agreements will contain a specific confidentiality clause

5. ACCESS CONTROLS

Manual records - Safe Haven : "A place to send or receive person identifiable information in a protected environment"

Definitions

Safe haven - The term 'Safe Haven' describes an agreed set of administrative procedures to ensure the safety and secure handling of confidential information. It can also be considered to be a location within the organisation where confidential information is both received and stored in a secure manner. Safe haven procedures should be in place in any location where confidential information is being received, held or communicated, especially where information is of a sensitive nature.

Personal information - Personal information is information which can identify a person – in which the person is the focus of the information and links that individual to details regarded as private e.g. name and address, name and home telephone number, etc.

Sensitive Personal Information - Sensitive personal information is where information contains details of an individual's:

- Health or physical condition
- Sexual orientation
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions

For this type of information even more stringent measures are employed within the Practice to ensure that the data remains secure.

Current safe haven procedures in place in the Practice

The Practice has 5 fax machines, 2 at Lister House and 1 each at the branch sites, Oakwood Medical Centre, Chellaston and Coleman Street. The faxes are located in the dedicated staff areas. These rooms can only be accessed by staff/ other authorised visitors using fob entry, and meet all relevant health & safety and security requirements.

The fax machine at Oakwood, Coleman Street is located in a back office room which are locked every night. This room is only accessible by staff/ other authorised visitors and meets all relevant health & safety and security requirements.

The GPs are expected to operate a 'clear desk' policy when consultations are finished, and rooms are checked by reception staff each evening and morning to ensure any patient identifiable information is filed away appropriately (or locked away in a general folder so that paper work can be discussed and actioned as appropriate by the relevant staff the following day).

The Reception areas at all sites are the responsibility of the Reception Manager who ensures staff clear away/ lock up files etc. at the end of each day – this forms part of the regularly reviewed 'end of day procedures'.

The Administration area is the responsibility of the Assistant Practice Manager who ensures that patient identifiable information is locked away at the end of each day. The Business Practice Manager ensures the same applies to their areas.

5.1. General information on faxes

There is a strong preference in the Practice not to use fax machines to transmit personal data of any description unless it is deemed absolutely necessary. If fax is required the following rules apply:

- The fax is sent to a safe location where only staff with a legitimate reason to view the information can access it.
- The sender is certain that the correct person will receive it and the fax number is correct.
- Staff members must notify the recipient you are sending a fax and ask them to confirm by telephone when it has been received.
- Care is taken in dialing the correct number.
- Confidential faxes are not left lying around for unauthorised persons to see.
- Only the minimum amount of personal information should be sent. Where possible the data should be anonymised or a unique identifier used, e.g. NHS number.
- When sending a fax with patient identifiable information a fax cover sheet is sent stating:

- Who the fax is from
- The name of the recipient
- The number of pages the fax contains (including the top copy)
- Notification of the recipient to contact the sender on the arrival of a fax
- Contain a suitable confidentiality clause which must be included on the top copy of the fax.

Misdirected faxes

Any fax received in error is to be returned to the sender and comply with the guidelines noted above. The contents must not be disclosed to any other parties without the sender's permission. Information received from a misdirected fax should be treated as highly confidential and should not be divulged to others. A misdirected fax can be received from either internal or external sources.

Unsolicited faxes

Unsolicited or unexpected faxes should be treated with care until the sender has been identified. Unsolicited faxes are becoming more common; however, they can look official and can lead to the disclosure of confidential information. Most of it is junk advertising material and should be ignored as it may encourage further faxes from the same source.

See also:\Policies and Protocols\RECEPTION protocols\RECEIVED FAXES

5.2 Incoming and outgoing Mail

All incoming and outgoing mail (or faxes) containing patient information marked 'Safe Haven' are handled discreetly and passed on to the correct recipient without the mail being opened or read.

All incoming mail containing patient identifiable information is opened upstairs in the Lister House administration area away from public spaces. All inbound mail is logged and date stamped and distributed as soon as possible.

All outgoing mail containing patient identifiable information (both internal and external) is sealed securely and marked private and confidential. Some particularly sensitive mail is marked 'for the addressee only'.

5.3 Transporting confidential and sensitive documents

The designated owners of documents which contain confidential and sensitive information are responsible for ensuring sufficient measures taken to protect their confidentiality, security and integrity during and after transportation or transmission.

When selecting the most suitable delivery option for documents the Practice pays particular attention to the information classification level and to any possible security risk such as mishandling and misuses, and the potential for theft inherent in each delivery option, delivery medium and delivery location.

- If the transport medium is inappropriate for the sensitivity or value of the information, being transported, it could facilitate the theft of the contents while in transit.
- If the transport medium used does not protect confidential data or does not protect from transit damage, information may be lost or at least delayed.
- Electronic transport methods may expose or damage confidential data in transit.

5.4 Sending Patient Identifiable Information Electronically

For guidance on sending patient identifiable information electronically staff should refer to the 'Transfer of Patient Records' policy.

5.5 Storage of Patient Identifiable Information

- To be held in a lockable/ pass only access area
- Filing cabinets locked. Consulting 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
- 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

5.6 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

5.7 General Guidance

- Visitor log maintained
- Confidential conversations conducted relative to the security of the environment. If the information being given is confidential but irrelevant the caller must be stopped. Ensure that the person is who they say they are.
- Original medical records not released to third parties
- Emailing of patient data sent ONLY from NHS.net email addresses and sent only to a restricted list of email addresses approved on the home page of the nhs.net email system - both sender and receiver must have the correct domain at the end of the e-mail address. Current known approved domains are: gsi.gov.uk, gse.gov.uk, gsx.gov.uk, mod.uk, pnn.police.uk, scn.gov.uk, cjsm.net, gcsx.gov.uk, nhs.net
- Or place the information inside a password protected attachment and phone the password through to the person you are sending the document to. DO NOT SEND IN THE EMAIL.

5.7 Freedom of Information

- The Act gives the general right of access to all types of "recorded" information (e.g. e-mails, policies, minutes etc) held by public bodies, sets out exemptions and places a number of obligations on public bodies.

5.8 Who can apply for information?

- Anyone, any individual or organisation anywhere in the world (and in any language) can apply for information.

- The application must be a recognised transaction e.g. letter or e-mail
- State name & address for correspondence
- Describe the information required.

6 Records management

The Practice is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal. This will ensure that the Practice can control the quality and quantity of the information that it generates, can maintain that information in an effective manner, and can dispose of the information efficiently when it is no longer required.

The Practice's clinical system (TPP SystmOne) contains vital records on which patient care and service provision depend. The Practice will ensure that staff are fully aware of the measures that are necessary to comply with current Information Governance best practice.

The Practice is also registered for the *Data Protection Act* (the Data Protection Officer is the current Business Practice Manager).

7 Data Protection Guidelines – 8 Basic Principles (SEE APPENDIX C)

Personal data must be:

- **Processed fairly & lawfully**
- **Processed for limited & lawful purposes**
- **Adequate, relevant & not excessive**
- **Accurate & up-to-date**
- **Kept for no longer than necessary**
- **Processed in line with the data subject's rights**
- **Kept secure**
- **Not transferred outside the EEA without protection**

What practical measures can we take to ensure confidentiality of patient information?

- Do not discuss patient information outside work
- Don't discuss patient information in public areas.
- Do not leave patient identifiable information in view of others
- Dispose of confidential waste either by using a shredder or confidential waste bins.
- NHS Records Management Code of Practice specifies the minimum length of time records should be retained.

8. NHS Confidentiality Code of Practice *c*overs situations when information can be disclosed without consent:

1. In an emergency
2. In the public interest e.g. contagious diseases have to be reported
3. Legal requirements (by statute or court order)
4. To protect third parties e.g. child abuse
5. Sectioned under the Mental Health Act

9. Training and awareness

The Practice will ensure that staff have the appropriate levels of awareness and training to comply with the Information Governance policy. All new staff receive Information Governance awareness training as part of their induction and are asked to sign a document confirming they understand the core principles we work to.

There is an ongoing programme of training using the IG Training Tool at www.igte-learning.connectingforhealth.nhs.uk/igte/ or the Bluestream GP Practice E-learning suite. Information on who has undertaken training using this tool is available on the Practice Training Log.

10. Legal compliance

The Practice has established measures to ensure compliance with the laws governing information use. The main laws relating to Information Governance are listed in Appendix A.

Staff should have the appropriate level of understanding of the relevant laws and of the measures that should be taken to comply with them.

11. Patient Confidentiality Statement

All patient information is considered to be confidential and we comply fully with the Data Protection Act. All employees have access to this information in relation to their role and have signed a confidentiality agreement. Information may be shared, in confidence, with other NHS organisations in the interests of patient care.

The Organisation's Responsibilities

The organisation will ensure that employees fully understand all their responsibilities with regard to confidential data. The employees will sign a written statement of the responsibilities they are undertaking towards the security of the data.

The organisation will also ensure that arrangements are in place for the confidential disposal of any paper waste generated at work or the employees' home.

The organisation will monitor and record when it is passing ownership of data to an individual (e.g. for project work or, research and development) and this will be individually and specifically authorised by the Caldicott Guardian. The individual may then need to be separately registered under the Data Protection Act 1998. The practice will otherwise fully comply with all aspects of data security as required under the Act.

The organisation will strictly apply the rules of confidentiality and in general will not release patient information to a third party without proper valid and informed consent, unless this is within the statutory exempted categories such as in the public interest, in which case the release of the information and the reasons for it will be individually and specifically documented and authorised by the responsible clinician.

CCTV is installed internally in public areas and externally for security. Recordings are used entirely at the discretion of the partners including provision of images to the police or other official bodies, and will otherwise comply with the Practice's Data Protection registration.

TELEPHONE CALLS

Please note that it is the Practice's policy to record all telephone calls for the purposes of patient and staff care, security, and dispute resolution. Recordings and their use will be at the Partners' discretion and will also comply with the Practice's Data Protection registration.

12. Breaches of confidentiality

All actual and potential breaches in confidentiality are expected to be disclosed to the line manager concerned as soon as possible via the Significant Event Process (see separate Significant Event Policy). The IG Lead (Dr

Brooks or Rachel Boldison) will then gather up relevant details and the issue will be investigated /reported according to the Data Breach Protocol Data Breach Reporting Policy - Shortcut.lnk. Any breach will also be addressed via the Practice's significant events process.

Appendix A: Guidance applying to Information Governance includes, but is not limited to the following:

Legal Acts that apply to Information Governance include:

- Common Law of Confidence
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- Computer Misuse Act 1990 (amended in 2005)
- Copyright, designs and patents Act 1988 (as amended by the Copyright Computer programs regulations 1992)
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Childrens Act 2004

NHS National Requirements

1. The NHS Confidentiality Code of Practice
2. The NHS Records Management Code of Practice
3. NHS Information Governance Toolkit guidance

Practice Related Policies/Protocols

We have the following protocols / policies in place to support Caldicott principles.

- **Dealing with Subject Access Requests Flowchart**
- **Clinical Governance Policy**
- **Computer Confidentiality, Internet and E mail Policy**
- **Confidentiality Agreements (various)**
- Professional codes of conduct from the BMA, GMC and NMC and others including Allied Health Professionals, Finance Professionals and NHS Managers
- **Significant Event Policy**
- **Smartcard Policy**
- **Appendix B - PRACTICE AUDIT MODEL**
-
-

ITEM	*Acceptable*	*Satisfactory*
Information provided to patients on the use of their information	An Information campaign exists on the website, and in posters and in leaflets to promote understanding of NHS information requirements	
Staff Code of Conduct for Confidentiality	Code of Conduct exists and staff are aware of it	Code reviewed and updated as required
Staff Induction procedures	IG Information Sheet provided at induction and signed by new starters.	IG Information Sheet provided at induction and signed by new starters.
Information Governance training needs	Systematic assessment of staff training needs and evaluation of training.	Staff training needs are for annual IG training. Evaluation has also concluded that the Caldicott Guardian (and SIRO) receives additional training on the role of the Caldicott/IG Lead in and NHS Information Risk Management for SIROs and IAOs.
Training Provisions (confidentiality and security)	Confidentiality policy signed at induction.	All staff to receive IG and GDPR training at appropriate levels and timeframes as defined in document S:\C81072\Departments\BPM\Rachel\Training\IG GDPR and Safeguarding Training core standards

		Summary for Managers.docx Training completed in Bluestream Training Tool or F2F for Caldicott guardians
Staff Contracts		Confidentiality included in all staff contracts
Contracts with other organisations	Confidentiality Agreements included in the signing in book.	
Reviewing information flows containing patient identifiable information	Information flows have been mapped.	
Safe haven procedures in place to safeguard information flows into the Practice		Safe haven in place for all patient identifiable information
Information Governance responsibility	An appropriately trained Information Governance Lead is in place	
Security incidents		Significant Event Procedures are documented and accessible to staff to ensure incidents are investigated promptly
Security monitoring	Reporting of incidents or problems areas takes place.	
User responsibilities		Password changes enforced on a regular basis
Controlling access to confidential patient information	SystmOne Access for staff is role specific and auditable. Some physical controls ie: Door Entry System. Staff vigilance also relied upon to control access.	

APPENDIX C

Seven golden rules for information sharing

Extract from HM Government *Information Sharing: Guidance for practitioners and managers.*
Copies can be obtained from **www.ecm.gov.uk/informationsharing**

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only

with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

APPENDIX D: USEFUL LINKS

Should you require further advice or guidance with reference to Information Governance or Information Security please contact Dr Brooks, Rachel Boldison or the Arden & GEM CSU Information Governance Team.

Information Governance Policy Intranet Page
http://sdccgintranet.wordpress.com/policies/governance/

Information Governance Training via the Health and Social Care Information Centre IG Training Tool.
https://www.igtt.hscic.gov.uk/igte/index.cfm

Records Management: NHS Code of Practice
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

Confidentiality: NHS Code of Practice
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Guide to Confidentiality in Health and Social Care
http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

Caldicott 2 Report: Information: To Share or Not to Share – The Information Governance Review
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Information Commissioners Office
http://www.ico.org.uk

Information Sharing: Guidance for practitioners and managers.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277834/information_sharing_guidance_for_practitioners_and_managers.pdf

Information Sharing: Guidance for practitioners and managers.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277834/information_sharing_guidance_for_practitioners_and_managers.pdf

APPENDIX E: FLOWCHART OF KEY QUESTIONS FOR INFORMATION SHARING

Does the information satisfy all of these points: Justifiable, Necessary, Secure, The Minimum Amount Needed, To be seen only on a need to know basis, at risk of being seen by inappropriate persons, legally and ethically received or required.

If in any doubt, ALWAYS seek the advice of the Caldicott Guardian (Dr Brooks