Somerset Partnership NHS
NHS Foundation Trust

CONFIDENTIALITY AND DATA PROTECTION POLICY

Version:	5
Date issued:	**August 2017**
Review date:	**June 2018**
Applies to:	All Trust Staff and anyone acting on behalf of the Trust who has access to personal data

This document is available in other formats, including easy read summary versions and other languages upon request. Should you require this please contact the Equality and Diversity Lead on 01278 432000

DOCUMENT CONTROL

Reference	**Version**	**Status**	**Author**
PA/Aug 15/CP	5	Final	Information Governance & Records Manager

Amendments

Annual review of the policy and to include the latest changes to Health and Social Care Information Centre, Department of Health and NHS England guidance and any change to UK legislation.

Policy extended to September 2017.

Due review: policy updated to comply with the revised policy template, updated titles and groups following the revised Governance Structure and correct Caldicott Guardian. CIGG approved but to be reviewed within one year to consider GDRP.

Document objectives: To ensure Trust staff and those working on behalf of the Trust comply with Data Protection requirements.

Approving body	Caldicott and Information Group	Date: June 2017
Equality Impact Assessment	Impact Part 1	Date: August 2017
Ratification Body	Senior Management Team	Date: August 2017
Date of issue	**August 2017**	
Review date	**June 2018**	
Contact for review	Information Governance and Records Manager	
Lead Director	Director of Strategy and Corporate Affairs	

CONTRIBUTION LIST Key individuals involved in developing the document

Designation or Group
Information Governance and Records Manager
Caldicott and Information Governance Group
Senior Management Team
Equality and Diversity Lead

CONTENTS

Section	Summary of Section	Page
Doc	Document Control	**2**
Cont	Contents	**3**
1	Introduction	**4**
2	Purpose & Scope	**4**
3	Duties and Responsibilities	**5**
4	Definitions	**7**
5	Procedure	**8**
	Confidentiality and Data Sharing Procedures	**9**
	Sharing information between organisations	**10**
	Health Record Confidentiality Requirements	**10**
6	Reporting Data Breaches	**12**
7	Training Requirements	**12**
8	Monitoring Compliance and Effectiveness	**12**
9	References, Acknowledgements and Associated documents	**13**
10	Appendices	**14**
Appendix A	Data Protection Act 1998 principles	**15**
Appendix B	Revised Caldicott principles and Article 8 of the Human Rights Act 1998	**16**
Appendix C	Confidential Information and specific rules	**19**
Appendix D	Confidentiality Agreement form for patients and volunteers	**25**
Appendix E	Information Governance Toolkit Serious Incident Reporting Investigation	**26**
Appendix E	IG SIRI Initial Score Check	**28**
Appendix G	IG SIRI Assessment Mechanism	**31**

1. INTRODUCTION

1.1 This policy sets out the issues that staff need to be aware of and take into account when using patient, staff or other confidential or sensitive information.

1.2 This policy relates to:

- Electronic Patient Records (EPR),
- Paper health records,
- Staff records,
- Trust systems that hold personal confidential data (PCD)

1.3. This policy should be read in conjunction with the Trust's Information Sharing Protocols.

2. PURPOSE & SCOPE

2.1. The contents of this document apply to everyone working for or on behalf of the Trust working with personal confidential data including bank staff, agency/locum workers as well as those working for the organisation in a voluntary or honorary capacity.

2.1.2 This includes contractors and employees of partner agencies where contractual arrangements are in place as well as patient, carer, elected person, appointed and public representatives who take part in Trust committees and working groups, the Council of Governors and its committees and working groups and includes where information is held that was verbally communicated information into correspondence, written or written and transmitted through any form of electronic media and other information of a confidential nature which may be kept by the Trust.

2.2. For ease of reference the term "Staff" is used to encompass all those classes of individuals identified within paragraph 2.1 above.

2.3. All staff must ensure that all patients, staff and other personal confidential data held by the Trust remains confidential and they comply with the requirements of the Data Protection Act 1998.

2.4 This policy takes into account the revised Caldicott 2 principles adopted by the Department of Health and includes the new principle on information sharing (principle 7).

2.4.1 The (new) Seventh Caldicott principle confirms information sharing is legitimate and provides clinicians and others with the clear requirement that:

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 (Caldicott) principles. They should be supported by the policies of their employers, regulators and professional bodies.

3. DUTIES AND RESPONSIBLITIES

3.1 **Trust Board:** The Trust Board has overall responsibility for ensuring robust operational management systems and governance are in place in order for the Trust to be able to comply with the Data Protection Act 1998 and the general law on matters of confidentiality.

3.2 **Chief Executive**: The Chief Executive has the ultimate responsibility for compliance with the Data Protection Act 1998 for the Trust and for the confidential information held under that Act. As such the Chief Executive shall:

- appoint a Data Protection Officer
- appoint a Caldicott Guardian

3.3 **Data Protection Officer: The Director of Strategy and Corporate Affairs** is the Lead Director for Data Protection who will ensure that the Trust complies with the Data Protection Act 1998, maintain the Trust's Data Protection registration with the Information Commissioner's Officer and lead on the data protection work programme, in collaboration with the Caldicott Guardian.

3.4 **Caldicott Guardian: Consultant Psychiatrist** is the Caldicott Guardian who will lead on all aspects of Caldicott work across the Trust including confidentiality of patient information as required by the Caldicott principles and role of the NHS Caldicott Guardian.

3.4.1 Key Responsibilities of the Caldicott Function:

- to support the Caldicott Guardian.
- to ensure the data protection work programme as outlined above is successfully co-ordinated and implemented.
- to ensure the Trust complies with the principles contained within the NHS Code of Practice (Confidentiality) and that staff are made aware of individual responsibilities through policy, procedure and training.
- complete (in collaboration with the Data Protection Officer) the Confidentiality and Data Protection Assurance component of the Information Governance Toolkit, contributing to the annual assessment.
- provide routine reports to the Trust's Information Governance Steering Group on Confidentiality and Data Protection issues.

The Caldicott Function includes:

- obtaining advice from the Caldicott Guardian and as required external sources on Data Protection and Caldicott issues, for instance; Trust solicitors, Information Commissioners Office.
- receiving applications for disclosure of personal information, advising staff, patients and their representatives (as required) on disclosure(s).

3.5 **Data Protection Lead Manager:** The Head of Risk will be the lead manager on Data Protection, supported by the Information Governance and Records

Manager, Information Governance Officer and the Clinical Records Keeping Administrator: who between the three of them, together with the Caldicott Guardian, undertake the Caldicott Function role.

3.6 **All Staff:** All staff **have a duty to maintain the confidence of people's information.** This duty is required and must be complied with (conferred and owed) by common law, statute of law, contract of employment, disciplinary codes and policies (of which this is one) and professional registration.

All Trust staff: all staff who hold, obtain, record, use and store Trust information should be aware of their own personal responsibilities in ensuring that data/information is protected. They should:

- adhere to all Trust policies and procedures and guidance issued by the Department of Health;
- comply with the Law;
- manage and handle personal confidential data professionally and understand that they are responsible for adherence to the Data Protection Act 1998;
- ensure, where required, everyone managing and handling personal confidential data is appropriately trained to do so and appropriately supervised as required;
- know how to respond to anybody wanting to make enquiries about handling personal confidential data and the process for dealing with queries about handling personal information;
- be aware that regular reviews and audits are carried out in respect of the way personal confidential data is managed;
- attend the Trust approved designated training and awareness programmes and in particular Mandatory Training

Trust responsibilities: the Trust will through appropriate management, and strict application of criteria and controls:

- ensure the principles of the Data Protection Act 1998 and the revised Caldicott 2 principles are observed and followed, these can be found in appendix A.
- fully observe conditions regarding the fair collection and use of information.
- meet its legal obligations to specify the purposes for which information is used.
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- ensure the quality and integrity of information used.

- ensure that the rights of people about whom information is held can be fully exercised under the Act. This includes the right:
  - to be informed that processing is being undertaken
  - to be made aware processes are in place to access their personal information
  - to prevent processing in certain circumstances
  - to rectify, block or erase information which is regarded as factually inaccurate information
  - to be assured appropriate technical and organisational security measures are in place to safeguard personal information;
  - to be assured that personal confidential data is not transferred abroad without suitable safeguards.

4. DEFINITIONS

- **EPR:** Electronic Patient Record
- **StEIS:** Strategic Executive Information System
- **Data Protection Act 1998:** Only applies to living persons both for service use health records and staff personnel records. There are eight principles – see Appendix A.
- **Data Protection Breaches**: A deliberate or reckless breach is defined in Appendix C. Under the Data Protection Act 1998, health and staff records being disclosed must be checked for third party or serious harm information that cannot be disclosed. Failure to properly do so (deliberate negligence) may result in an investigation under this policy.
- **Access to Health Records Act 1990:** Only applies to deceased patient health records.
- **Human Rights Act 1998:** Applies especially in regards to Article 8: Everyone has the right to respect for his private and family life, his home and his correspondence.
- **Freedom of Information Act 2000:** UK public organisations must comply with this act. It allows for disclosure of public held information but restrictions (called exemptions) are available and may occur for personal confidential data under section 40 of that act.
- **Personal Confidential Data:** This is a term used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes dead as well as living people.

  The review interpreted 'personal' as including the Data Protection Act definition of personal data, but included data relating to the deceased as well as living people, and 'confidential' includes both information 'given

in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

Examples of identifiable data are:

- Name
- Address
- Postcode
- Date of Birth
- NHS Number

What is Personal Data?

As per the Data Protection Act 1998, and defined by the ICO:

Personal data means data which relate to a living individual who can be identified:

a. from those data, or

b. from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

What is Sensitive Personal Data?

Sensitive personal data is different from Personal Data. Sensitive personal data means personal data consisting of information as to:

a. the racial or ethnic origin of the data subject,

b. their political opinions,

c. their religious beliefs or other beliefs of a similar nature,

d. whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

e. their physical or mental health or condition,

f. their sexual life,

g. the commission or alleged commission of any offence, or

h. any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

5. PROCEDURE FOR THE DISCLOSURE OF PERSONAL RECORDS

5.1 The full procedure for disclosure of patient information is found in the Record Keeping and Records Management Policy. The main principles of that policy will also apply to staff wishing to have access to their staff files.

5.2 For ease of understanding, disclosures can be placed into two categories;

- Individual letters and other individual items.
- Complete health/staff record or multiple sections/letters.

5.3 Requests for complete copies of records (patient or staff), or multiple sections, or multiple letters, constitute a full application.

5.4 Where staff are concerned there may be a disadvantage by adhering to the duty of confidence principle too strictly, the Caldicott Guardian, the Data Protection Officer or the Corporate Governance team can provide advice.

5.4.1 All staff should be aware that any refusal to disclose information may be time limited. That is, it may only apply while there is an ongoing issue and once this has been resolved, the information may/may not be disclosable to the applicant or others.

- For third party information, only those third party entries that cannot be disclosed should be taken out (redacted). The remainder of the record is disclosable as normal.
- All staff should bear in mind the following:
  - it is not acceptable to withhold a full record where there are third party issues, simply because of the third party information.
  - on very limited occasions it may be that due to a very serious issue raised by the clinical team that advice is required on withholding all or most of the health record of a patient and not disclosing that record/record entries. Trust advice must be sought through the Corporate Governance Team if this is considered.

5.5 Unauthorised access, use or disclosure may be in breach of the Data Protection Act, the Human Rights Act, and/or breach Trust policies and may lead to disciplinary action. This is in addition to the statutory personal liability for deliberate or reckless breaches as stated above.

5.6 Breaches of confidentiality may also be reported to professional bodies for consideration, for example: General Medical Council, Nurses and Midwives Council, General Social Care Council.

CONFIDENTIALITY AND DATA SHARING PROCEDURES

5.7 Confidentiality means not disclosing any personal or sensitive information to any person who is not entitled to receive it, without either:

a. the consent from the person to whom the information relates or,

b. it is legally required to provide that information (e.g. Court Order or Safeguarding) or,

c. it is in the vital interests of the person (e.g. continuation of treatment) or, to protect the public (e.g. violent incident).

5.8 The revised Caldicott (2) principles which are approved by the Department of Health provide clear guidance on information sharing. They are found in full in Appendix B together with samples on usage.

Sharing Information between organisations

5.9 Information sharing between statutory/partner organisations directly involved in a patient's care and for the purpose of providing that care is essential to good practice. General consent from the patient for such information sharing of this sort, or agreed restrictions should be recorded following a discussion with the patient and written consent (or otherwise).

5.10 There is an expectation by the Information Commissioner's Office that data sharing will take place and endorses this providing it does not put the information at risk through loss of data. That is, legitimate sharing of information is permissible but losing that information while sharing it, is not.

5.11 The principle of sharing information in the interest of public safety is endorsed by the Trust, as long as it is only information that needs to be shared and only with those who have a clear need to know.

5.12 The Trust needs to collect and use certain types of information about a variety of people including, but not limited to:

- current, past and prospective employees
- suppliers and external agencies
- patients, clients, customers

5.13 In addition, the Trust is required to collect and use certain types of information for statistical analysis and data returns to comply with the requirements of Government departments, such as the Department of Health. Where this personal confidential data is collected, recorded and used, whether electronic or manual, it must be dealt with appropriately in line with Information Governance requirements.

5.14 To ensure that the Trust treats personal confidential data lawfully and correctly, it will fully endorse and adhere to the Principles of Data Protection, as set out in the Data Protection Act 1998 and found in appendix A.

Health Record confidentiality requirements

5.15 In all instances, NHS complaints and claims correspondence must not be uploaded into the electronic health record system, nor must full details of individuals' finances be uploaded unless agreed with the Finance department for the Trust.

5.16 It is important to establish as soon as possible the patient's wishes in respect of information sharing and confirm this by setting the colour (or in other record systems using equivalent mechanisms) in electronic health record, noting the following definitions;

- **Green**: information about the patient can be shared on a need to know basis with others involved with the patient's care, their immediate family

or partner as well as staff from other organisations directly involved in the patient's care (unless the client tells us otherwise).

- **Red**: The patient does not give consent to information being shared with one or more named people or organisations, or;
- Clinical staff are aware of specific issues where information should not be shared which the patient is unaware of, or has agreed to disclosure but that disclosure is not in the patients best interest, then the consent should be set to red until the risk has passed, Trust Management overrides the clinical decision, or a Court Order requires disclosure.

5.17 All patients should be given a copy of the confidentiality leaflet, which describes the traffic light system in advance of discussion about the setting of their traffic light.

5.18 **Inpatients (all Divisions)** should be asked within 24 hours of admission, unless clinically unable to give informed consent and in that case the Confidentiality flag should be set to red. If someone remains unable to give consent for longer than one calendar month from admission, the consultant (Responsible Clinician) must state in the notes *either* that the patient lacks capacity to consent *or* lacks sufficient understanding of the issue to be able to make a decision *or* refuses to discuss consent issues.

5.19 **Community patients (all Divisions)** should normally be asked within 5 working days and in all cases within one month of first appointment.

5.20 When the Red flag (limited consent) is used, a note should be added in the comments box to identify the specifics of the lack of consent(s), for example, 'not to family member 'X'. This then applies to all information including paper health records, unless overruled by law.

5.21 Where a confidentiality statement is set to (or changed to) Red, this must be reviewed at least annually. On admission to an in-patient ward, the patient should be asked at the earliest opportunity, and in all circumstances within one month unless clinically unable to do so, to confirm if it should remain at Red, and, if so, whether the accompanying statement of limitation is still correct.

5.22 In all cases, the Trust will abide by Red confidentiality statements set in electronic health record unless:

- the information is the subject of a Court Order
- the information is needed for the prevention or detection of crime
- there are child protection safeguarding issues

5.23 If the client lacks capacity to consent to disclosure, a *Best Interests Checklist* must be completed, which may conclude that information may be shared, and the traffic light recorded as Green. Please refer to the Trust Consent and Capacity to Consent to Treatment Policy for further guidance regarding incapacity and best interests.

5.24 Where patient information is being used for legal (or similar) purposes the patient should sign a separate specific consent for this, normally supplied by

their solicitor or advocate, and the patient should understand that the information may be used in an open Court of Law. This may apply without the knowledge or consent of the patient when in relation to a Court Order, the prevention of crime or child protection issues.

5.25 If there is doubt about sharing information with external bodies, written consent should be sought. If this is not appropriate, the duty to share must be discussed with the line manager and either the Caldicott Guardian, Director of Strategy and Corporate Affairs, Head of Risk or the Information Governance and Records Manager.

6. REPORTING DATA BREACHES

6.1 Reporting any confidentiality breach will be through the Trust's DATIX electronic untoward incident reporting system.

6.2 All breaches of confidentiality will be collated by the Trust's Caldicott Guardian assisted by the Caldicott Function and will be presented to, and reviewed by, the Caldicott and Information Governance Group.

6.3 If there appears to have been a significant breach of confidentiality or the legislation then this should be immediately reported to the Data Protection Officer or the Caldicott Guardian so that reporting to the relevant regulatory body (Department of Health, Information Commissioner) through the new Information Governance SIRI reporting tool within the Information Governance Toolkit can take place.

7. TRAINING REQUIREMENTS

7.1 The Trust will work towards all staff being appropriately trained in line with the organisation's Staff Training Matrix (training needs analysis). All training documents referred to in this policy are accessible to staff within the Learning and Development Section of the Trust Intranet.

7.2 Training is provided at the Corporate Induction and on a Mandatory annual basis through use of the e-learning Information Governance Toolkit Training modules(s).

8. MONITORING COMPLIANCE AND EFFECTIVENESS

8.1. Monitoring arrangements for compliance and effectiveness

Overall monitoring will be by the Caldicott and Information Governance Group

8.2. Responsibilities for conducting the monitoring

The Caldicott and Information Governance Group will monitor procedural document compliance and effectiveness.

8.3. Methodology to be used for monitoring

- random sampling of staff and by questionnaire
- internal audit

- external auditor investigations and reports
- complaints monitoring
- incident reporting and monitoring
- clinical effectiveness monitoring

8.4. **Frequency of monitoring**

Quarterly reports to the Caldicott and Information Governance Group in the form of an Information Security breach log.

9. REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

9.1 **References**

Data Protection Act 1998

Human Rights Act 1998

Access to Records Act 1990

Public Records Act 1958

Freedom of Information Act 2000

Computer Misuse Act 1990

Copyright, Designs and Patents Act 1988

Confidentiality: NHS Code of Practice 2003

Caldicott Guardian Manual 2006

Caldicott Review 2012

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation May 2015

9.2 **Cross reference to other procedural documents**

Consent and Capacity to Consent to Treatment Policy

Freedom of Information Policy

Information Security Policy

Record Keeping and Records Management Policy

Risk Management Policy and Procedure

Untoward Event Reporting Policy and procedure

All current policies and procedures are accessible in the policy section of the public website (on the home page, click on ‘Policies and Procedures’). Trust Guidance is accessible to staff on the Trust Intranet.

10. APPENDICES

10.1 For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such.

Appendix A	Data Protection Act 1998 principles
Appendix B	Revised Caldicott principles and Article 8 of the Human Rights Act 1998
Appendix C	Confidential Information and specific rules
Appendix D	Confidentially Agreement form for patients and volunteers
Appendix E	Information Governance Toolkit Serious Incident Requiring Investigation (SIRI)
Appendix F	IG SIRI Initial Score Check
Appendix G	IG-SIRI Assessment Mechanism

APPENDIX A

DATA PROTECTION ACT 1998 PRINCIPLES:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and
   in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

APPENDIX B

REVISED CALDICOTT PRINCIPLES ARE:

(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.

Trust note: this means all staff handling personal confidential data must be able to justify why they have accessed and used this information. You must meet the Trust's ''Legitimate Relationship'' requirements.

(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).

Trust note: this means staff must think carefully about what information they are using and why. It also means that any subsequent use of that information must also be taken into account.

(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.

Trust note: Do not disclose information because 'it might be useful' – there must be a clear reason for adding that information in any use or disclosure.

(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.

Trust note: RiO Electronic health record is the main record management system used by the Trust and can adjust access rights accordingly. This note *applies to all Trust systems that hold personal confidential data* whether patient, staff or others.

Staff need to be aware that sometimes there will be a clear need to know of the 'bigger picture' and two examples are:

a. patient is seen in Minor Injuries Unit (MIU) a week after leaving General Hospital having had surgery for leg/foot injury. The MIU identify that the Podiatrist should review the patient as well as a Pain Clinic. The Pain Clinic identify that the patient is also depressed because of the effects of the accident (bicycle) and refer the patient to the Community Mental Health Team.
b. Staff details are held on the Trust's Electronic Staff Record which are accessed by Human Resources and Payroll. The member of staff has a long term sick-note from their GP and both HR and Payroll need access to this to ensure correct salary payment(s) are made. The member of staff's line manager is also informed.
c. For both the above (a and b) the Legitimate Relationship must be met. Any member of staff who does not meet this requirement is accessing information outside of this and acting outside this Caldicott principle.

(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.

Trust note: all staff are required to comply with Trust policies that apply to them. All staff will have a contract and this will include Information Governance and Confidentiality statements. All staff are required to complete the Information Governance training (Mandatory) yearly.

(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.

Trust note: The key lead staff are noted in section 3 of this policy.

(7) (The new principle): 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.

Trust note: There has been no change or amendment to the Data Protection Act 1998 as information sharing is already permitted. This new Caldicott principle identifies that in many instances where information could have been shared, it was not. The Information Commissioners Office is clear in that

legitimate information sharing is both legal and good practice but the loss of that information (during or after that sharing) is not.

THE FIVE RULES - HEALTH AND SOCIAL CARE INFORMATION CENTRE

The five rules of patient confidentiality, set out in the new Health and Social Care Information Centre guidance are:

1. Confidential information about patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

THE HUMAN RIGHTS ACT 1998 ARTICLE 8:

ARTICLE 8 RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

APPENDIX C

Confidential Information and specific rules

Information on Trust sensitive and/or confidential information

- Information within this policy will be broadly divided into;
- Patient information
- Staff information
- Information relating to the Trust including;
    - Notes of confidential meetings
    - Confidential and privileged information
    - Records of complaints and investigations

Confidentiality means not disclosing any personal or sensitive information to any person who is not entitled to receive it, without either:

a. the consent from the person to whom the information relates or,

b. it is legally required to provide that information (e.g. Court Order or Safeguarding) or, it is in the vital interests of the person (e.g. continuation of treatment) or, to protect the public (e.g. violent incident).

Where the person to whom the information relates has given their permission for the information to be disclosed then disclosure of this information would not amount to a breach of confidentiality.

Equally, if the information is already in the public domain, or is already known to the recipient of the information, it *may not* amount to a breach of confidentiality. However, great care should be taken not to repeat information given by another source, as this might still amount to a breach of confidence or possibly it may be defamatory.

In practice, clinical and social care staff will outline the boundaries and extent of confidentiality with patients, and should do so at an early stage. For example, the keeping of confidentiality within a team or a service is entirely acceptable and appropriate disclosure to other staff involved in a patient's care would not amount to a breach of confidentiality. Equally, information sharing between statutory organisations is permitted within the Data Protection Act.

People have the right to expect that:

- Personal confidential data held about them is not accessed, used or disclosed improperly.
- The sharing of their information with other NHS Trusts and Organisations complies with the law

The same duty of confidentiality and Data Protection requirements applies to personal confidential data about staff except more senior staff whose names and job titles may be disclosed, e.g. Information about Directors, which is published and is therefore a matter of public record or contact information of Trust Managers.

No employee shall inappropriately access, misuse or share any information or allow others to do so. Staff are personally liable for deliberate or reckless breaches of the Data Protection Act and may be liable to disciplinary action and/or prosecution.

Any personal confidential data given or received in confidence for one purpose may not generally be used for a different purpose, or passed to anyone else without the consent of the provider of the information.

Any member of staff who invites a volunteer, user or carer to participate in any activity of the Trust must ensure that responsibilities in respect of confidential information are discussed as early as possible. All such volunteers, users and carers must sign a confidentiality statement (see Appendix D). If there is any doubt as to the status of an individual volunteer, user or carer in terms of their ability to receive confidential information then advice should be sought from Human Resources department and/or the Information Governance and Records Manager.

When is it acceptable to breach confidentiality?

There is a clear public interest in the maintenance of confidentiality, breaching confidentiality can harm the patient, third parties and damage the patient-professional relationship and the Public perception of professionals. However, on occasions it is necessary to breach confidentiality where there is a greater public interest in doing so. This balancing test is sometimes referred to as the "Egdel test". A clear example of a permissible breach of confidentiality would be where a patient tells a staff member that a third party is at real risk of harm. In these circumstances it is good practice to try and persuade the person to agree to the disclosure of this information. Consideration should be given as to whether an interpreter or translator should be required in these circumstances.

However, if they do not agree then it is good practice to inform the person of the extent of the disclosure that will be made by the staff member and the reasons why. The decision making process and the discussions with the person involved should be documented in the patient's electronic record. It is recommended that the staff member seeks advice from their supervisor and/or line manager before making a confidential disclosure and where necessary this decision should be the subject of a multi-disciplinary risk assessment. Should there be any doubt about the need to make a confidential disclosure then advice should be sought from the Caldicott Guardian. Staff should also refer to professional guidance i.e. GMC, NMC, GSCC, and other Allied Professional Bodies including UKIP. All such breaches in confidentiality must be reported on the DATIX system and will be reviewed and scrutinised by the Caldicott and Information Governance Group.

Where it is not acceptable to breach confidentiality:

A deliberate breach of confidentiality will be when either or both of the above definitions are broken, without good reason and not in the vital interest of the patient or other persons at significant risk.

A negligent breach is where information is disclosed because the failure to adhere to policy and process and the breach takes place by virtue of being negligent and not acting properly.

A reckless breach of confidentiality is breaking any of the above but without malice or deliberate intent, but where the member of staff has been thoughtless or reckless in causing a breach.

Additionally for staff, the accidental viewing and further disclosure of personal information, or obtaining of personal confidential data that you are not entitled to know may constitute a breach of the second principle of the Data Protection Act 1998.

The Trust is clear that an avoidable breach of confidentiality is unacceptable and may well result in disciplinary action. However, the Trust also accepts that there are

degrees of breach from accidental and inadvertent acts through to deliberate and malicious acts. A proportionate but fair response needs to influence any applications of the Trust's disciplinary procedures.

Equally the Trust wishes to encourage open and transparent reporting of harm related incidents and as such it considers self reporting to be of primary importance for this who have made a mistake and breached confidentiality.

The duty of confidentiality remains even after staff leave Trust employment.

The above points also apply to staff personal confidential data as held by the Trust.

The systemic breach of confidentiality

The Trust is greatly concerned about systemic breaches of confidentiality. There have been high profile public examples of breaches in confidentiality through the misplacing of patient information on laptops, data devices and storage devices. It is vital that these breaches are reported immediately but more importantly, measures are put into place to prevent them happening wherever possible in the first place.

As a result of these concerns the following rules are set out for staff:

i. Patient information and patient identifiable information must only be recorded on Trust approved systems and in line with the Trust's Information Technology and Management Security Policy.

ii. Patient pseudo-anonymised information or commercially or organisationally sensitive information must only be held on prescribed Trust drives or in line with the Trust's Information Technology and Management Security Policy.

iii. All Trust laptops, Blackberry's and mobile data storage devices must be encrypted and supplied by the Trust. Active cards are provided for those who require access to confidential information remotely and advice should be sought from the appropriate service manager as to the service requirements for technology to support lone working.

iv. Paper patient records must be created, used and stored in line with the Trust's Record Keeping and Records Management Policy.

v. Where a patient's records require a pseudonym, advice should be sought from the Caldicott Guardian. In general this should be considered where a patient is a close relative of a member of staff, is a member of staff themselves or for some other substantial reason that the Caldicott Guardian considers necessary.

vi. Paper diaries, where necessary for staff based in any community setting should only record patient's initials indicating patient appointments and should never include patient's full names or addresses.

1). Patient information

This is subject to the requirements of both the Caldicott Principles and the Data Protection Act 1998. Non-approved disclosure of patient information will be treated as a serious breach of confidentiality, unless mitigating circumstances prevail. Staff may be liable to disciplinary action including dismissal.

Patient information will be held so that no unintentional disclosure can take place and in line with Data Protection Act 1998 and records management principles and best practice.

Trust approved disclosures will only take place in line with the Data Protection Act 1998 and Caldicott principles, or as required by law, e.g. court summons/child protection.

2). Staff information

This is subject to the Data Protection Act and employment legislation as well as certain fiscal legislation.

Staff information will be held so that no unintentional disclosure can take place and in line with Data Protection Act 1998 and records management best practice and principles.

Staff may apply to have/view a copy of their staff record in line with Data Protection Act 1998 principles and regulations, which are the same as for patients.

Staff information will only be disclosed providing it is in line with the Data Protection Act, or required by statute of law, e.g. fiscal policy; statutory tax returns/child maintenance.

3) Information relating to the Trust

The Trust reserves the right to have confidential meetings where information is discussed and then held securely and confidentially. Information held and/or disclosed will not contravene the Freedom of Information Act 2000 or the Data Protection Act 1998.

The Trust also reserves the right to have confidential and privileged information which may include; legally privileged, relating to the Houses of Commons or Lords, or other such privileged information. Information held and if disclosed will not contravene the Freedom of Information Act 2000 or the Data Protection Act 1998.

Complaints and Investigations

Complaints and investigations are treated confidentially and remain so unless there is a legal requirement to release information. Information held and/or disclosed will not contravene the Freedom of Information Act 2000 or the Data Protection Act 1998, or other legislation that may apply, e.g. investigation leading to the Trust being required to disclose information to the police under the Crime and Disorders Act 1998.

All staff should note that complaints are processed separately to health records and NHS complaints, even from patients, should not be uploaded in to the electronic health record system.

When Information may be passed on

Information may be passed to someone else;

With the patient's consent or on a "need to know" basis if the recipient needs the information because they are concerned with the patient's care or if the information is needed for;

- Assuring and improving the quality of care and treatment
- Monitoring and protecting public health coordinating NHS care with other agencies (e.g. local authorities)
- Effective healthcare administration (e.g. managing and planning services)
- Contracting for NHS services (e.g. payment of staff)
- Auditing NHS accounts (auditors)

- Risk Management (e.g. health and safety)
- Investigating complaints and legal claims
- Teaching (within the NHS system)
- Statistical analysis or research*
- Statute or Court Order requires the information.
- Passing on information can be justified for other reasons (protection of the public)

* Specific consent should be sought for any activity relating to teaching or research that will involve people personally.

In any circumstances, staff who are unsure whether it is appropriate to disclose information should contact the Caldicott Guardian or Director of Finance and Business Development or the Information Governance and Records Manager for further advice.

General Information

All records which are created/added to by staff in the course of their work, in all media - paper, electronic, audio and video - are covered by this Code. All records created /added to by staff in the course of work are the property of the Trust, or, for social workers, the property of the County Council, unless the member of staff is working on behalf of the Trust. This includes diaries, which should be returned to the Human Resources Department on termination of employment.

Safeguards in respect of patient identifiable information:

- Before any patient information is divulged, staff should verify the identity of the person requesting it, establish that the information is required for a valid purpose, and check whether it could be anonymised and still be useful.
- Patient information should only be divulged to a third party if this is in the patient's interest, or for the treatment of the patient, or where the patient's consent has been obtained. Exception to this may be made when this is in the public interest, or where the Children Act or Crime and Disorder Act apply. Staff should refer to the Child Protection Handbook where child protection issues are concerned.
- Staff working in the IT Department must ensure that they comply with the additional issues covered in the IM&T Security Policy, Section 10 – Housekeeping.

If patient identifiable information has to be posted from Trust premises or transferred between units, it is the sender's responsibility to ensure that all reasonable precautions are taken to ensure that the information is securely wrapped and hidden from view. Transit envelopes must **not** be used.

Staff should be mindful at all times that manual and electronic records must be kept secure – they should not be left on desks in open, unoccupied rooms.

When transporting case notes, patient related correspondence, or laptop computers, care must be taken that these are well-wrapped, carried in the car boot, and not left in an unattended vehicle.

It is not permissible to take case notes/records of one patient into anther patient's home.

Staff must ensure that records are securely stored out of sight when a room is left unattended, or when 'unauthorised to view' people are present. This includes workmen, patients, patients' relatives, visitors and members of staff who do not need access to the information. Computer screens should not display patient information under these circumstances.

No employee is allowed to keep patient identifiable information in a personal database, either paper or electronic, without prior consent from the Director of Governance and Corporate Development and the Caldicott Guardian. Failure to obtain permission will result in a breach of the Data Protection Act.

Audit and Research

If any patient identifiable information is to be used in research, then the Research and Development policy must be followed.

Trust Audits involving patient or staff personal information.

The Trust is required as part of its legitimate work to complete audits relating to either patient or staff personal confidential data in order to comply with regulatory activity. This will include but not limited to:

- Information Governance Toolkit audits: clinical and non-clinical
- Record Management audits of clinical records
- Clinical audits required by regulatory bodies
- Audits required by the Audit Commission
- Audits required by the Department of Health

All formal Trust Audit activity must comply with the requirements of the Data Protection Act 1998 where access to patient, staff other people's information is made.

The Trust will ensure that all such audits are Trust approved and have mechanisms in place to validate the audit, the outcomes and recommendations.

APPENDIX D

Somerset Partnership NHS Foundation Trust

CONFIDENTIALITY AGREEMENT FORM

Confidentiality Statement for patients and volunteers

The Trust is committed to empowering patients, and one initiative is for patients/ex-patients or volunteers to join in with Trust activities, including membership of formal Trust Groups (Committee meetings) and other activities.

In these circumstances information may be discussed or read by patients or volunteers which is;

- Not for disclosure.
- Not for disclosure at the meeting but may be published later.
- Not for disclosure until approved by the Trust Board or the Executive Team.

Patients and volunteers who join or have joined any formal Trust activity must have their attention drawn to the confidential nature of the activities or the Trust Group and be responsible for their own actions.

Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the Data Protection Act 1998 or an action for civil damages under the same Act.

Patients or volunteers who join groups, meetings or activities should always consider the information to be confidential unless specifically informed otherwise by the Chair of a group, Director, Trust senior manager, or member of staff acting on behalf of a Trust Director or senior manager.

No information of a personal nature shall be given out by the patient or volunteer in respect of a request under the Freedom of Information Act 2000. Advice on any FOI request will be sought from the Information Governance and Records Manager.

By signing this agreement, the signatory agrees to abide by the Somerset Partnership NHS Foundation Trust Confidentiality and Data Protection Act policy.

_____ _____

Signed Dated

_____ _____

Witnessed (Trust Senior Manager or designate) Dated

APPENDIX E

Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation

Managing and Investigating Information Governance Serious Incidents Requiring investigation

- All Information Governance Serious Incidents that require investigation must be reported through the Connecting for Health: Information Governance Toolkit via the Trust's Corporate Governance Team.
- The first thing to do then is decide if it requires investigation.

PROCEDURES

- The Trust uses Datix as its primary reporting mechanism and once an information governance concern or breach is reported the Head of Risk or the Information Governance and Records Manager will review this and decide if it requires reporting to Connecting for Health (IGT) as an Information Governance Serious Incident Requiring Investigation (IG-SIRI)
- The Health and Social Care Information Centre (on behalf of the Department of Health) believe that an IG – SIRI is:
    - Any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 1998 and/or the Common Law of Confidentiality.
    - This includes unlawful disclosure or misuse of confidential data, recording or invasion or people's privacy.
    - Such personal data breaches which could lead to identity fraud or have other significant impact on individuals
    - Applies irrespective of the media involved and includes both electronic media and paper records.
- These incidents may immediately become apparent that they are IG-SIRI's or, as more information becomes available they may turn into an IG-SIRI.
- It is vitally important that any person involved in reviewing whether the incident meets an actual or potential breach of law is capable of making such a decision and the Trust confirms the following staff are approved for this:
    - Director of Strategy and Corporate Affairs – Data Protection Officer
    - Head of Risk – Data Protection Manager
    - Information Governance Manager – Data Protection Technical Advisor
    - Information Technology Technical Architect – Information Security Manager
- The Head of Risk and the Information Governance and Records Manager both have access to the Trust's Information Governance Toolkit including the IG-SIRI Reporting Tool.

- The IG-SIRI score system in Appendix F is to be used by the reviewers to gain an idea of score and impact – known as scale and sensitivity.
- The flow chart in Appendix G is to be used to determine whether an IG-SIRI has occurred and if it requires reporting or not via the IGT IG-SIRI mechanism.

Contact Person	**Information Governance and Records Manager**

Information Security

This guidance requires assessment and confirmation of information security compliance by the Trust's Information Security Manager.

Compliance checked	**September 2013**
Information Security Manager	**Information Technology Technical Architect**

APPENDIX F

The following process should be followed to categorise an IG SIRI

Step 1: Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point.

Baseline Scale (existing)	
0	Information about less than 11 individuals
1	Information about 11-50 individuals
1	Information about 51-100 individuals
2	Information about 101-300 individuals
2	Information about 301 – 500 individuals
2	Information about 501 – 1,000 individuals
3	Information about 1,001 – 5,000 individuals
3	Information about 5,001 – 10,000 individuals
3	Information about 10,001 – 100,000 individuals
3	Information about 100,001 + individuals

Step 2: Identify which sensitivity characteristics may apply and the baseline scale point will adjust accordingly.

Sensitivity Factors (SF) modify baseline scale	
Low:	**For each of the following factors reduce the baseline score by 1**
-1 for each	(A) No sensitive personal data (as defined by the Data Protection Act 1998) at risk nor data to which a duty of confidence is owed
	(B) Information readily accessible or already in the public domain or would be made available under access to information legislation e.g. Freedom of Information Act 2000
	(C) Information unlikely to identify individual(s)

High:	For each of the following factors increase the baseline score by 1
+1 for each	(D) Detailed information at risk e.g. clinical/care case notes, social care notes
	(E) High risk confidential information
	(F) One or more previous incidents of a similar type in the past 12 months
	(G) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information
	(H) Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual
	(I) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment
	(J) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident

The Incident Reporting Tool will not allow you to select sensitivity factors which would not be relevant based on initial selections. See below for settings and key for A to J sensitivity factors noted above.

When user selects this:	The following sensitivity factors are excluded:
A	D, E
B	D, E, I, J
C	I,J
D	A, B
E	A, B
F	Nothing excluded
G	Nothing excluded
H	Nothing excluded
I	B, C
J	B, C

Step 3: Where adjusted scale indicates that the incident is level 2, the incident should be reported to the ICO and DH within the reporting timescales noted in this guidance. There is a 'notify later' option within the IG Incident Reporting Tool which can be used to save the incident for a short period to allow you to seek authorisation from local Senior Management or Data Protection Officer to report to Regulators/Central Bodies, if required.

Final Score	Level of SIRI
1 or less	Level 1 IG SIRI (Not Reportable)
2 or more	Level 2 IG SIRI (Reportable)

APPENDIX G

IG-SIRI Assessment Mechanism