Somerset Partnership NHS
NHS Foundation Trust

Privacy Impact Assessment Policy

Version:	1
Ratified by:	Senior Managers Operational Group
Date ratified:	August 2015
Title of originator/author:	Information Governance & Records Manager
Title of responsible committee/group:	Caldicott & Information Governance Group
Date issued:	**August 2015**
Review date:	**July 2018**
Relevant Staff Groups:	Information Asset Owners

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 Number PA/Aug15/PIA	**Version** 1	**Status** Final	**Author** Information Governance Manager
Amendments	Included amendments suggested from Caldicott and Information Governance group members,		
Document objectives: To enable the Trusts Information Asset Owners (IAOs) to address the privacy concerns and risks, a technique referred to as Privacy Impact Assessment (PIA), as advocated by the Information Commissioners Office.			
Intended recipients: Senior and Team Managers who are IAOs.			
Committee/Group Consulted: Caldicott and Information Governance Group.			
Monitoring arrangements and indicators: Information Governance Toolkit requirements monitored through the Caldicott and Information Governance Group.			
Training/resource implications: General awareness for all Trust staff. Specific training from the Information Governance Team for IAOs and IAAs.			
Approving body and date	Caldicott & Information Governance Group	Date: May 2015	
Formal Impact Assessment	Impact Part 1	Date: August 2015	
Clinical Audit Standards	N/A	Date: N/A	
Ratification Body and date	Senior Managers Operational Group	Date: August 2015	
Date of issue	**August 2015**		
Review date	**July 2018**		
Contact for review	Information Governance and Records Manager		
Lead Director	Director of Governance and Corporate Development		

CONTRIBUTION LIST Key individuals involved in developing the document

Name	Designation or Group
Phil Brice	Director of Governance and Corporate Development
Tricia Oliver	Information Governance Officer
Kurt Hanson	Information Security Manager
Sue Flynn	Head of IM & T
Group Members	Caldicott and Information Governance Group
David Nation	Information Development Architect
Andrew Sinclair	EIA / Head of Corporate Business

Contents

CONTENTS

1. INTRODUCTION

1.1 The Government's Data Handling Review report contains a number of recommendations that are mandatory to the wider public sector. Part of the solution to reducing risk lies in on-going culture change to ensure that Information Risk Management is high on the agenda and the process of Privacy Impact Assessment (PIA) is advocated as a means of achieving this.

1.2 This PIA policy is applicable to any member of staff who are responsible for project managing a new "project" or "plan" to modify any existing system (information asset).

1.3 **NEW** projects that involve personal confidential data or intrusive technologies give rise to privacy issues and concerns. Privacy embraces "confidentiality" and "patient consent" and as an overarching principle this policy advocates that respect for patient privacy and dignity should be considered at the outset of any project, which embraces confidentiality and patient consent. To enable an organisation to address the privacy concerns and risks, a technique referred to as Privacy Impact Assessment (PIA), as advocated by the Information Commissioner, **must** be used.

1.4 This policy has been developed from the Information Commissioner's Office (ICO) in their 'Privacy Impact Assessment Handbook version 2.0'.

1.5 As we are an NHS organisation we are registered under the Data Protection Act 1998 with the ICO as data controller for "processing personal information to enable us to provide healthcare services". Therefore we process patients and staff information which is classified as Personal Confidential Data (PCD) and sensitive data.

1.6 As an NHS organisation therefore we must comply with the Data Protection Act 1998 and other UK Privacy Laws when we process such information. Therefore no screening process as mentioned in the ICO PIA handbook need be completed. Therefore for all information systems new or currently in place a small-scale PIA will be completed first. This will then be followed by a Full-scale PIA.

Small-scale PIA

1.7 Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project'

Full-scale PIA

1.8 Conducts a more in-depth internal assessment of privacy risks and liabilities. Analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them.

1.9 Privacy Impact Assessment guidance is provided for staff members by the Information Governance Team, as part of the Information Asset Owner training. The Information Governance team is also responsible for ensuring support and guidance is given when staff members are required to fill out the Privacy Impact Assessment.

2. PURPOSE

2.1 The aim of a Privacy impact Assessment is to ensure that systems and processes within the Trust are fit for purpose and include privacy by design. The confidentiality and the protection of the information within the information asset **must** be assessed. There must also be a comprehensive consideration of potential impacts on information quality and security at the design phase of any new process or procurement of a new information asset.

Privacy by design

2.2 Benefits of taking a 'privacy by design' approach:

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

3. SCOPE

3.1 The scope of this document is to outline the Trust's approach and methodology for Privacy Impact Assessments for, current systems that have not had a PIA before and also **NEW** systems.

3.2 It covers all information assets that are paper or electronic within the Trust.

3.3 This Policy covers all staff employed by the Trust, private contractors, volunteers and temporary staff.

3.4 The term "Trust" includes all Somerset Partnership NHS Foundation Trust services.

4. EXPLANATIONS OF TERMS USED

4.1 **Privacy Impact Assessment** – (PIA's) A risk technique advocated by the ICO to enable organisations to address privacy concerns and ensure appropriate safeguards are addressed and built in as projects or plans to develop existing information assets.

4.2 **Projects / plans to develop** – PIA's are required when new projects occur (for example introduction of a new electronic patient record) or where plans are proposed to develop an existing information asset. These can be both paper and electronic.

4.3 **Sensitive Data** – under the Data Protection Act 1998 is data for example such as patient diagnosis, medical history, ethnicity, sex, religion.

4.4 **Personal Confidential Data** – is data for example such as name, postcode, GP, next of kin, address, date of birth etc.

4.5 **Information Asset –** An Information Asset is Service User, staff or corporate information / data, processed by us and is held in an electronic or hard copy/manual format. Therefore we are the data controller.

4.6 **Accreditation of Information Assets** – The small scale and full scale PIA will form part of the accreditation documentation for an Information Asset.

5. DUTIES AND RESPONSIBILITIES

5.1 The adherence to the PIA Policy and procedures is essential for assuring aspects of the Information Governance agenda, this is maintained and supported by

Trust Board

5.2 In his communications with NHS Trusts Chief Executives, the NHS Chief Executive has made it clear that ultimate responsibility for Information Governance in the NHS rests with the Board of each organisation.

Chief Executive

5.3 The Trust's Accountable Officer is the Chief Executive who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risk is handled in a similar manner to other risks such as financial, legal and reputational risks.

5.4 Reference to the management of information risks and associated information governance practice is now required in the Statement of Internal Control which the Accounting Officer is required to sign annually.

SIRO (Senior Information Risk Owner)

5.5 The SIRO is the Director of Finance and Business Development. The SIRO is an executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

The role:

- is accountable
- fosters a culture for protecting and using data
- provides a focal point for managing information risk and incidents
- is concerned with the management of all information assets.

Information Governance and Records Manager

5.6 The Information Governance Manager is responsible for ensuring the organisation meets its statutory and corporate responsibilities and is also accountable for:

- ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance;
- ensuring that in line with the IG Checklist appropriate measures are taken to ensure that adequate consideration is given to the Privacy Impact Assessment;
- providing support for staff members required to complete the PIA by providing Information Asset Owner Training and further support to complete the PIA as deemed necessary.

Information Asset Owners (IAO) – Directors, Heads of Service, Matrons, Ward Managers and Service and Team Managers

5.7 The SIRO is supported by departmental / section IAOs who are senior managers involved in running the relevant services. Their role is to understand what information is held, what is added, and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to information assets they "own" and to provide assurance to the SIRO on the security and use of the assets.

Information Asset Administrators (IAA)

5.8 IAA's work with an information asset on a day to day basis. They have day to day responsibility, ensure that policies and procedures are followed by staff and recognise actual or potential security incidents, and consult their IAO on incidents. They may also be known as the Application Manager for an Information System.

Information Security

5.9 The Head of IM&T (with delegated responsibility to the Information Security Manager) is responsible for the provision and management of a high quality, customer focussed, Information Technology Security Advisory Service using expertise to manage security issues, identifying best practice and making recommendations for local implementation.

6. PIA MANANGEMENT PROCESS

The Information Asset Management Process and the PIA

6.1 Privacy Impact Assessments need to be completed at an early stage of the project BEFORE the new 'proposed' system is procured or BEFORE the planned 'change' has taken place as part of the Information Asset Management Process.

6.2 The next section illustrates the important stages and/or information for consideration when looking at procuring new systems or changing those already used by the Trust. The aim is to ensure that all elements of a project that may impact upon the ability of the Trust to protect its data are being considered.

7. PIA PROCESS

7.1 The appointed Information Asset Owner is responsible for ensuring the PIA is completed and that the PIA is carried out with support and guidance from other individuals as relevant, i.e. Information Governance Team, Information Security.

The following process **must** be followed:

STEP 1

a. Inform appropriate Leads (Directors / Heads of Division) on the process for New System / Process or Proposed change to an Information System. Communication is essential to ensure compliance with checklist and processes.

STEP 2

a. Information Governance Lead will start the Accreditation of Information Asset documentation by forwarding this policy to the Information Asset Owner.

b. Initial Information Governance Security Checklist to be carried out by the Information Asset Owner / Information Asset Administrator. (*SMALL SCALE PIA*)

c. c PIA will be carried out, supported by Information Governance. If an electronic system is involved, advice and support from the IT Services Information Security Lead.

d. Once identified that the system holds Person Confidential Data and Sensitive Data, full scale PIA to be completed, with the support of the Information Governance Team.

e. Where non-compliance is identified in the small / full scale PIA then risk assessments completed, risks highlighted to SIRO where required.

STEP 3

a. a Procurement Process starts; informed by results of IT and IG checks and PIA.

b. An action plan for ensuring PIAs are embedded in the Life Cycle of the Information Asset.

c. Information Governance and Records Manager will progress Accreditation Information Asset document in line with the development of the project.

d. Information Governance will ensure that all Accreditation of Information Asset documents are approved by the Caldicott and Information Governance Group and a process of audit and review is put in place.

7.2 In following this process and ensuring that Information Governance are notified and involved from the initial conception of the project we can provide

assurance the Trusts information is being handled in a secure and responsible way and complies with UK Law.

Note: The PIA is only applicable where the proposed new project/system/process or proposed change to a system/process is to use personal confidential data (PCD) along with sensitive data, or significantly change the way in which personal data is handled

7.3 As a result of a completed Privacy Impact Assessment an action plan must be devised and written up for initial approval and subsequent auditing and monitoring by the Caldicott and Information Governance Group.

7.4 This ensures that information risks are recorded, mitigation put in place with an annual review to ensure on-going compliance with confidentiality, data protection and security.

Please follow the procedure laid down in Appendix A of this document to complete the PIA.

8. TRAINING

8.1 Guidance on the nature of the Privacy Impact Assessments will be provided to Information Asset Owners and Administrators. This will involve bespoke training by the Information Governance Team called “Information Asset Owner Training”.

8.2 All Information Asset Owners (IAOs) will be made aware of their responsibilities for the protection of their Information Assets through generic and specific training programmes and guidance.

8.3 IAOs need to have an understanding of:

- what a privacy impact assessment is and what information assets to apply it to;
- what information assets they are responsible for;
- when to apply a PIA;
- how it links into the procurement or implementation of a new system;
- how to incorporate the action plans into a project plan;
- knowing who to contact to get advice and guidance.

9. EQUALITY IMPACT ASSESSMENT

All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected characteristics as defined by the Equality Act 2010. In addition, the Trust has identified Learning Disabilities as an additional tenth protected characteristic. If you, or any other groups, believe you are disadvantaged by anything contained in this document please contact the Equality and Diversity Lead who will then actively respond to the enquiry.

10. MONITORING COMPLIANCE AND EFFECTIVNESS

10.1 Overall monitoring will be the responsibility of the Caldicott and Information Governance Group who receive quarterly reports from the Information Governance and Records Manager. The Caldicott and Information Governance Group will provide a six monthly progress report to the Integrated Governance Committee using the Governance Reporting Template.

Process for Monitoring Compliance

10.2 Overall monitoring will be the responsibility of the Caldicott and Information Governance Group who receive quarterly reports, including monitoring, from the Information Governance and Records Manager.

Monitoring will be through:

- Action Plans from PIA;
- Risk Assessment Action Plans;
- Project Risk and Issues logs;
- Audit of PIA process on an annual basis;
- Audit of PIA documentation.

10.3 Shortfalls identified will be discussed at the Caldicott and Information Governance Group and Action Plan(s) devised. The Caldicott and Information Governance Group will provide a six monthly progress report to the Integrated Governance Committee using the Reporting Template.

10.4 The Clinical and Social Care Effectiveness Group will, as required, provide reports to the Clinical Governance Group using the Governance Reporting Template.

10.5 Lessons learnt will be noted by the Caldicott and Information Governance Group within the report to the Integrated Governance Committee.

11. COUNTER FRAUD

The Trust is committed to the NHS Protect Counter Fraud Policy – to reduce fraud in the NHS to a minimum, keep it at that level and put funds stolen by fraud back into patient care. Therefore, consideration has been given to the inclusion of guidance with regard to the potential for fraud and corruption to occur and what action should be taken in such circumstances during the development of this procedural document.

12. RELEVANT CARE QUALITY COMMISSION (CQC) – Registration Standards

12.1 Under the **Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (Part 3), the fundamental standards** which inform this procedural document, are set out in the following regulations:

Regulation 11:	Need for consent
Regulation 13:	Safeguarding service users from abuse and improper treatment
Regulation 15:	Premises and equipment

Regulation 17:	Good governance
Regulation 20:	Duty of candour
Regulation 20A:	Requirement as to display of performance assessments.

12.2 Under the **CQC (Registration) Regulations 2009 (Part 4)** the requirements which inform this procedural document are set out in the following regulations:

Regulation 18:	Notification of other incidents

12.3 Detailed guidance on meeting the requirements can be found at http://www.cqc.org.uk/sites/default/files/20150311%20Guidance%20for%20providers%20on%20meeting%20the%20regulations%20FINAL%20FOR%20PUBLISHING.pdf

12.4 Relevant National Requirements

NHS Records Management
Information Governance Toolkit
Public Records Act 1958
Freedom of Information Act 2000

13. REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

13.1 References

- Department of Health. (April 2007). Information Security Management: NHS Code of Practice. London: Department of Health. Available at: www.dh.gov.uk
- Department of Health. (2006). Records Management: NHS Code Of Practice Part 1 and Part 2. London: Department of Health. Available at: www.dh.gov.uk
- Data Protection Act 1998. London: The Stationery Office. Freedom of Information Act 2000. London: The Stationery Office.
- NHS Connecting for Health Information Governance Toolkit 2015 (Version 13)
- Department of Health Records Management: NHS Code Of Practice (2009)
- HMSO Data Protection Act 1998 (1998)
- Information Commissioners Office Privacy Impact Assessment Handbook version 2 (2010)

13.2 Cross reference to other procedural documents

Confidentiality and Data Protection Policy
DATIX Risk Register Guidance
Development & Management of Procedural Documents
Freedom of Information Policy
Information Security Policy
Risk Management Policy and Procedures

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.

14. APPENDICES

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 – Procedure for PIA

APPENDIX A

PROCEDURE FOR PIA

The aim of a Privacy Impact Assessment is to ensure that systems and processes within the Trust are fit for purpose. Some of the considerations that must be taken into account are whether a new (or modified) project /process or information asset will:

- Ensure the necessary consents have been obtained from those whose personal data is being used;
- Affect the quality of personal information already collected;
- Allow personal information to be checked for relevancy, accuracy and validity;
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required in line with Department of Health retention and destruction guidelines;
- Have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction, breaches of confidentiality or damage;
- Enable data retrieval to support business continuity in the event of emergencies or disasters;
- Enable the timely location and retrieval of personal information to meet subject access requests;
- Alter the way in which the organisation records in or monitors and reports information from a key organisational system.

Please double Click on the link below which will open up the SOMPAR PIA assessment spreadsheet. The spreadsheet includes instructions on how to complete the PIA.

Please complete as much as you can and seek Information Governance Team advice when you run in to problems:

Information Governance & Records Manager

Information Governance Team
Somerset Partnership NHS Foundation Trust
2nd Floor, Mallard Court, Express Park, Bristol Road,
Bridgwater, Somerset TA6 4RN

Tel: 01278 432075
Mobile: 07789920502