Livewell Southwest

Privacy Impact Assessment Policy & Procedure

Version No. 1.2

Notice to staff using a paper copy of this guidance

The policies and procedures page of the Intranet holds the most recent version of this guidance. Staff must ensure they are using the most recent guidance.

Author:	**Information Governance Group**
Asset Number:	**823**

Reader Information

Title	**Privacy Impact Assessment Policy & Procedure. V.1.2**
Asset number	823
Rights of access	Public
Type of paper	Policy and procedure
Document purpose/summary	Privacy Impact Assessment is a process which will assist the organisation in ensuring that privacy concerns and safeguards are addressed and built in as projects and systems are introduced.
Author	Information Governance Group
Ratification date and group	24th February 2016. Policy Ratification Group
Publication date	3rd March 2016
Review date and frequency (one, two or three years based on risk assessment)	Three years after publication, or earlier if minor changes are required.
Disposal date	The PRG will retain an e-signed copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or withdrawn from circulation.
Job title	Information Governance Lead
Target Audience	All LSW staff, contractors and partner organisations working on behalf of LSW that introduce new processes or systems that are likely to involve a new use or significantly change to the way in which personal data is handled.
Circulation List	Electronic: Livewell Southwest (LSW) intranet and website (if applicable) Written: Upon request to the PRG Secretary on ☏ 01752 435104. Please contact the author if you require this document in an alternative format.
Consultation Process	Information Governance Group
Equality analysis checklist completed	Yes
References/sources of information	DH Governance Toolkit - https://nww.igt.hscic.gov.uk/ Cumbria Partnership NHS Foundation Trust PIA Policy (2011) Information Commissioner's Office Privacy Impact Assessment Handbook V.2 (2009) – www.ico.gov.uk DH: NHS IG - Information Risk Management - Good Practice Guide 2009 Data Protection Act 1998
Associated documentation	• Information Governance Policy • Communications Systems: Phone, Email,

	Internet & Fax Policy • Records Management Policy • Clinical Record & Note Keeping • IT Security Policy • Data Protection, Confidentiality, Caldicott & Safe Haven Policy • Information Sharing Policy • Risk Management Policy • Disclosure of Health Records
Supersedes document	v.1.1
Author contact details	By post: Local Care Centre Mount Gould Hospital, 200 Mount Gould Road, Plymouth, Devon. PL4 7PY. Tel: 0845 155 8085, Fax: 01752 272522 (LCC Reception).

Document review history

Version no.	**Type of change**	**Date**	**Originator of change**	**Description of change**
0.1	New document	27/2/13	Information Governance Lead	New document
1.1	Update	24/9/14	Information Governance Lead	Minor changes to titles.
1.2	Review	Dec 2015	Internal Audit	No changes, updated to Livewell.

Privacy Impact Assessment Policy & Procedure

1 Introduction

1.1 This policy sits within Livewell Southwest (LSW) Information Governance Framework, and is based on guidance set out by the Information Commissioner's Office (ICO) Privacy Impact Assessment (PIA) Handbook (July 2009). It explains how LSW will manage assurance in relation to privacy, confidentiality and data protection requirements for all new projects and systems that are introduced to the organisation.

1.2 With so much information being collected, used and shared in the provision of healthcare, it is important that steps are taken to protect the privacy of each individual and ensure that personal information is handled legally, securely, efficiently and effectively in order to deliver the best possible care.

1.3 Conducting a PIA is also a requirement set out in the Information Governance Toolkit – a Department of Health (DH) mechanism that the Health and Social Care Information Centre (HSCIC) is commissioned to develop and maintain.

2 Purpose

2.1 The purpose of conducting a PIA is to:

- Meet and exceed legal requirements.
- Identify and manage risks to address any privacy issues.
- Avoid loss of trust and reputation by minimising privacy deficiencies.
- Inform the organisation's communications strategy by consulting with stakeholders.
- Avoid unnecessary costs by performing a PIA at an early stage in project.
- Avoid 'bolt on' solutions which could be more expensive in the longer term.

3 Definitions

3.1 **Privacy Impact Assessment** – a process to identify and minimise the privacy risks associated with any new projects, processes or systems, and to ensure appropriate safeguards are addressed and built in. 'Privacy risks' are risks to the privacy of individuals whose personal information will be used on the system or affected by the change.

3.2 **Personal confidential information** is information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual last name or isolated postcode, or small pieces of different information which if taken together could allow the person to be identified. Examples of personal information are address, data of birth, name etc.

3.3 **Sensitive personal information** is usually treated confidentially and whose loss or misdirection could impact adversely on individuals, the organisation or on the wider community. Sensitive personal information is defined in the Data Protection Act 1998, and is where the personal information contains details of health or physical condition, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sexual life or criminal convictions.

4 Duties and responsibilities

4.1 The **Chief Executive** has overall responsibility for the strategic direction and operational management, including ensuring that LSW process documents comply with all legal, statutory and good practice guidance requirements.

4.2 The **Senior Information Risk Officer (SIRO)** [Director of Professional Practice, Safety & Quality] is responsible to the Board for ensuring Information Risk Policy is developed, implemented, reviewed and its effect monitored. Privacy Impact Assessment is one element of the management of information risk. Information risks needs to be handled in a similar manner to other major risks such as financial, legal and reputational risks.

4.3 **General staff responsibilities** - all LSW staff, contractors and partner organisations working on behalf of LSW must follow the requirements of this and related policies, particularly those relating to Information Governance. All health professionals must also meet their own professional codes of conduct in relation to confidentiality.

5 Procedure

5.1 When should I start a PIA?

5.1.1 A PIA is most effective when started at an early stage of a project or implementation of a new system. Ideally, it should be started before decisions are set in stone and systems have been procured. See appendix one for a PIA proforma for new projects or systems.

5.2 Who should conduct a PIA?

5.2.1 The person who is in a position to manage the risks and influence the design of the project, process or system should be responsible for undertaking the PIA e.g. it could be the manager responsible for the project. Whilst staff assigned with responsibility for Information Governance, Data Protection etc. may provide advice, they will not be responsible for completing the PIA.

5.3 Does a PIA need to be completed for every project or system?

5.3.1 Not every project or system will require a PIA. The ICO sees PIAs being used only where a project is of such a wide scope, or will use personal information of such a nature, that there would be genuine risks to the privacy of the individual. PIAs will usually be recommended where a change of the law will be required, new and intrusive technology is being used, or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way.

Examples:

- The implementation of a new patient information system.
- Replacement of an existing personal data system, with consequential changes to business processes and/or data storage.
- Enhancements to an existing system in order to collect, store and use several additional items of personal data.
- The re-design of web forms for capture of personal data from patients.

6 Training implications

6.1 The Information Governance Team will provide support and guidance in relation to information risk management and conducting a PIA in order to fulfil the obligations set out in this policy. If you require assistance please email LSWCIC.InformationGovernance@nhs.net or phone 01752 (4)34711.

7 Monitoring compliance and effectiveness

7.1 The policy’s effectiveness will be monitored and reviewed periodically through the Information Governance Group and the Information Governance Toolkit which will require an annual audit on the effectiveness of this policy and the quality of the assessments completed.

All policies are required to be electronically signed by the Lead Director. Proof of the electronic signature is stored in the policies database.

The Lead Director approves this document and any attached appendices. For operational policies this will be the Locality Manager.

The Executive signature is subject to the understanding that the policy owner has followed the organisation process for policy Ratification.

Signed: Director of Professional Practice, Safety & Quality

Date: 1st March 2016

Appendix one – Privacy impact assessment form for new projects and systems

Please read through all the questions thoroughly and answer with as much detail as possible. If you require any assistance, please contact the Information Governance Lead via the email address below. Once the form has been completed, please forward to IG LSWCIC.InformationGovernance@nhs.net for approval via the Information Governance Group.

General details

Project title:		**Contact details:**	
Project lead:		**Date**:	

Project Description: (summary of project and why it is required)	
Cross reference to other projects:	
Relationships: (e.g. other organisations involved)	
Customers and Stakeholders identified:	

PIA key questions

1. Will the project/system contain personal identifiable data or sensitive data? If no you do not need to complete any further as PIA not required.	**If yes, will it involve data for:** □ **Patients** □ **Staff** □ **Other (specify):**
2. Please state purpose for the collection of the data e.g. patient treatment, research, audit etc.	
3. Does the project/system involve new privacy intrusive technologies?	□ **Yes** □ **No** **If yes, please give details:**

4. Please tick the personal data items that relate to the project/system.	□ **Name** □ **Post Code** □ **GP** □ **Next of Kin** □ **Sex** □ **NI No.** □ **Address** □ **DOB** □ **Consultant** □ **NHS No.** □ **Hospital No.** □ **Tel. number** □ **Other**
5. Please tick the sensitive data items that relate to the project/system.	□ **Treatment dates** □ **Diagnosis** □ **Occupation** □ **Medical History** □ **Sexual life** □ **Religion** □ **Ethnic Origin**
6. Will the project/system collect new personal or sensitive data items which have not been collected before?	□ **Yes** □ **No** If yes, what is the new personal/sensitive data?
7. Have patients / staff provided consent for the processing of personal identifiable or sensitive data been informed of the new data collection / use of data?	□ **Yes** □ **No** If yes, state how they have been informed? E.g. leaflet, poster, website etc.
8. Will the information be shared with any other organisations?	□ **Yes** □ **No** If yes confirm that there is a Data Sharing Agreement in place or other appropriate protocols/measures to mitigate risks and ensure adequate level of security.
9. Have any information security arrangements changed? For example, security policies, backup policies, storage of data (either electronic or paper)?	□ **Yes** □ **No** If yes, please state changes below:
10. If applicable is the third party contract / supplier of the system registered with the Information Commissioner?	□ **Yes** □ **No** If yes, what is their Notification Number:
11. If applicable, does the third party / supplier contracts contain all the necessary Information Governance clauses?	□ **Yes** □ **No**
12. Has the method of transporting the information to, from and within the LSW changed?	□ **Yes** □ **No** If yes, please state how the information will be transported? E.g. email, phone, fax etc.

13. Does this transfer of information comply with the LSW’s Data Protection, Confidentiality, Caldicott & Safe Haven policy?	□ **Yes** □ **No**
14. Have all relevant departments been informed of the process/system?	□ **Yes** □ **No**
15. Has an information risk assessment been undertaken for the change in the system / process to address any issues?	□ **Yes** □ **No** If yes, please provide a copy of the risk assessment and ensure this is inputted on the risk register.

<u>To be completed by the Information Governance Group</u>

Comments:

Name:

Title:

Date: