NHS
Scarborough and Ryedale
Clinical Commissioning Group

Privacy Impact Assessment Standard Operating Procedure

Author	Embed Health Consortium
Date approved	June 2016
Committee	Information Governance Steering Group
Version	2.2
Review date	June 2018

Version history

Version	Date	Author	Description	Circulation
0.1	12/09/14	WSYBCSU	Initial Draft	IG Committee
2	12/08/15	YHCS	Minor revisions and clarifications added	IG Committee
2.1	06/09/16	Embed	To reflect Information Commissioners Guidance	IG Steering Group
2.2	26/06/17	Corporate Services Manager	Minor amends to formatting	

Contents

1 Introduction

Privacy Impact Assessments serve to ensure that the organisation remains complaint with legislation and NHS requirements such as the Information Governance Toolkit, which determine the use of Personal Confidential Data (PCD). The Information Governance Checklist and Privacy Impact Assessments (PIA) have been developed to provide an assessment prior to new services or new information processing/sharing systems being introduced. They are less effective when key decisions have already been taken.

Privacy Impact Assessments (PIAs) identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow for the identification and remedy problems at an early stage, reducing potential distress, subsequent complaints and the associated costs and damage to reputation which might otherwise occur.

A PIA aids an organisation in determining how a particular project, process or system will affect the privacy of the individual. It is important to consider whether a PIA is required once you know what it is you are hoping to achieve, what you will require to get there and how you plan to go about doing it.

Conducting a PIA does not have to be complex or time consuming.

2 Privacy Impact Assessments

PIAs help identify privacy risks, foresee problems and bring forward solutions. A successful PIA will:

- identify and manage risks (see Appendix A for examples)
- avoid inadequate solutions to privacy risks
- avoid unnecessary costs
- avoid loss of trust and reputation
- inform the organisation's communication strategy
- meet or exceed legal requirements

The Information Commissioners Office (ICO) has produced guidance materials on which this procedure is based (see Appendix C).

Consideration as to whether a PIA should be completed is mandated through the Information Governance Toolkit. PIAs ensure that privacy concerns have been considered and serve to assure the organisation regarding the security and confidentiality of the personal identifiable information.

4 Purpose of a PIA

A PIA should serve to:

- identify privacy risks to individuals
- identify privacy and Data Protection compliance liabilities
- protect the organisations reputation
- instil public trust and confidence in your project/product
- avoid expensive, inadequate “bolt-on” solutions
- inform your communications strategy

Following review of the screening questions (Annex A) it may be decided that a PIA is required. Where it is thought that a PIA is required, Annex B should be completed and submitted to the Information Governance Team for a preliminary review. It is recommended that the IG Team review is sought prior to the final PIA being submitted to the IG Committee (Leeds CCGs), SIRO or Caldicott Guardian.

5 Responsibilities

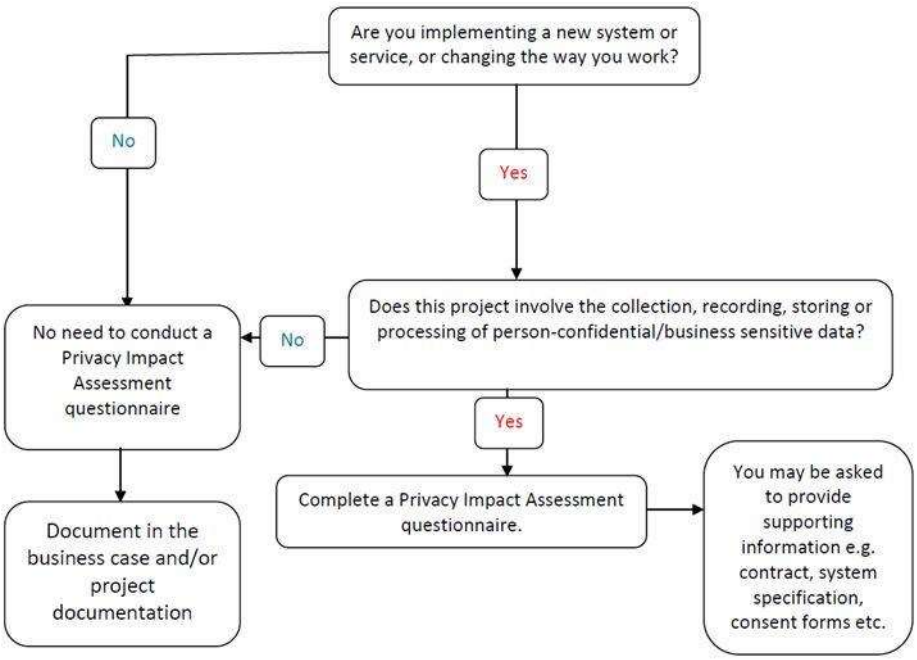
Responsibility for ensuring that a Privacy Impact Assessment is considered and if appropriate, completed, resides with managers leading the introduction of new systems, sharing or projects.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of the Privacy Impact Assessment procedure.

There is an expectation that partner organisations involved in supplying/providing services should provide technical information for the Privacy Impact Assessment, where this is otherwise unclear.

This guidance therefore applies to all staff and all types of information held by the organisation. Further details of responsibilities are to be found in the organisation’s policies and procedures.

6 Is a PIA required for every project?



The ICO envisages PIAs being used where a project includes the use of personal data, where there otherwise a risk to the privacy of the individual, utilisation of new or intrusive technology, 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. The screening questions (see Annex A) help determine if a PIA is required.

7 When should I start a PIA?

PIAs are most effective when they are started at an early stage of a project, when:

- the project is being designed
- you know what you want to do
- you know how you want to do it
- you know who else is involved

It **must** be completed before:

- decisions are set in stone
- you have procured systems
- you have signed contracts/Memorandum of Understanding/agreements
- while you can still change your mind

8 Publishing PIA's

All PIA's are to be included within the organisation's Publication Scheme and must therefore be presented to the Head of Governance once they have received approval.

It is acknowledged that PIA's may contain commercial sensitive information such as security measures or intended product development. It is acceptable for such items to be redacted but as much of the document should be published as possible given all information within a public organisation can be requested through the Freedom of Information Act and will be listed in the Publication Scheme.

9 Related CCG Policies

- Access to Records under DPA Procedure
- Business Continuity Plan
- Confidentiality and Data Protection Policy
- E mail Policy
- Freedom of Information and EIR Policy
- Freedom of Information Procedures
- IG Strategic Vision, Policy and Framework
- Incident Reporting Policy
- Information Security Policy
- Interagency Information Sharing Protocol
- Internet and Social Media Policies
- Network Security Policy
- Privacy Impact Assessment procedure
- Records Management and Information Lifecycle Policy
- Remote access and home working procedures
- Risk Management Policy
- Safe Haven Guidelines and Procedure

10 Appendix A - Example risks

10.1 Risks to individuals

a) Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
b) The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
c) New surveillance methods may be an unjustified intrusion on their privacy.
d) Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
e) The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.

f) Identifiers might be collected and linked which prevent people from using a service anonymously.
g) Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
h) Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
i) Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
j) If a retention period is not established information might be used for longer than necessary.

10.2 Corporate risks

a) Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
b) Problems which are only identified after the project has launched are more likely to require expensive fixes.
c) The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
d) Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
e) Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
f) Data losses which damage individuals could lead to claims for compensation.

10.3 Compliance risks

a) Non-compliance with the DPA.
b) Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
c) Non-compliance with sector specific legislation or standards.
d) Non-compliance with human rights legislation.

11 Appendix B - Glossary

Item	Definition
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Caldicott	Seven Caldicott Principles were established following the original reviewed in 1997 and further development in 2013. The principles include: justify the purpose(s) don't use patient identifiable information unless it is necessary use the minimum necessary patient-identifiable information access to patient identifiable information should be on a strict need-to-know basis everyone with access to patient identifiable information should be aware of their responsibilities understand and comply with the law the duty to share information can be as important as the duty to protect patient confidentiality

Item	Definition
Data Protection Act 1998	This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must: be processed fairly and lawfully. be obtained only for lawful purposes and not processed in any manner incompatible with those purposes. be adequate, relevant and not excessive. be accurate and current. not be retained for longer than necessary. be processed in accordance with the rights and freedoms of data subjects. be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. not be transferred to a country or territory outside the European Economic Area unless that country or territory protects the rights and freedoms of the data subjects.
European Economic Area (EEA)	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they ‘own’ and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.

Item	Definition
Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
Information Risk	An identified risk to any information asset that the organisation holds. Please see the Risk Policy for further information.
Personal Data	This means data which relates to a living individual which can be identified: from those data, or from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also 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
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.

Item	Definition
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Pseudonymisation	Where patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Records Management: NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Sensitive Data	This means personal data consisting of information as to the: racial or ethnic group of the individual the political opinions of the individual the religious beliefs or other beliefs of a similar nature of the individual whether the individual is a member of a trade union physical or mental health of the individual sexual life of the individual the commission or alleged commission by the individual of any offence any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board

12 Appendix C - Further information

12.1 Relevant statutory legislation and law:

- Common Law Duty of Confidentiality
- Data Protection Act 1998
- Freedom of Information Act 2000
- General Data Protection Regulations (draft)
- Human Rights Act 1998
- Privacy and Electronic Communications Regulations 2015

12.2 Further reading and guidance:

- Caldicott 2 Review Report and Recommendations
- Confidentiality Code of Practice
- HSCIC Code of practice on confidential information
- Information Security Code of Practice
- Records Management Code of Practice
- The ICO's Anonymisation: managing data protection risk code of practice may help identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing: code of practice may help to identify privacy risks associated with sharing personal data with other organisations.
- The ICO's Privacy Notices: Code of Practice.