University Hospitals Birmingham
NHS Foundation Trust

CONTROLLED DOCUMENT

Privacy Impact Assessment Procedure

CATEGORY:	Procedure
CLASSIFICATION:	Governance
PURPOSE	To identify at an early stage any privacy issues and implement privacy by design. This will ensure that the Trust meets its obligations under all relevant data protection legislation and also meets the expectations of individuals.
Controlled Document Number:	1015
Version Number:	002
Controlled Document Sponsor:	Director of Corporate Affairs
Controlled Document Lead:	Senior Manager Information Governance
Approved By:	Director of Corporate Affairs
On:	October 2017
Review Date:	October 2020
Distribution: • **Essential Reading for:** • **Information for:**	Project Managers, Divisional Management Teams, Senior Managers, Budget Holders All Staff

Contents

Paragraph		Page
1	Purpose	3
2	Scope	3
3	Process	3
4	References	11
5	Associated Policy and Procedural Documentation	11
Appendices		
Appendix A	Privacy Impact Assessment Template http://uhbpolicies/assets/PrivacyImpactAssessmentProcedureAppendixA.docx	
Appendix B	Access Control for Specified Systems http://uhbpolicies/assets/PrivacyImpactAssessmentProcedureAppendixB.docx	

1. Purpose

1.1. The purpose of a Privacy Impact Assessment (PIA) is to identify the most effective way to comply with data protection obligations and meet the expectations of individuals by implement privacy by design. This will ensure that University Hospitals Birmingham NHS Foundation Trust (the Trust) will avoid or rectify problems at an early stage, reducing the associated costs and damage to the Trust's reputation, which might otherwise occur.

1.2. Conducting a PIA supports the Trust obligations under all relevant data protection legislation i.e. UK Data Protection Act and EU GDPR.

1.3. This procedure sets out detailed instructions on how to complete a PIA.

1.4. This procedure may be amended from time to time by the authority of the Director of Corporate Affairs, provided that such amendments are compliant with the associated policies.

2. Scope

This procedure applies to all new projects, service developments, procedures and policies within the Trust that involve the processing of personal information will require screening using the Screening Questions.

3. Procedure

3.1. All new projects, procedures and policies that involve using or sharing personal information will require a completed Privacy Impact Assessment at the initial stages and prior to any deployment of system or procurement decision being made. Examples of these are when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals such as large scale processing of specific data or systematic processing activities that could have significant effects of individuals.

3.2. PIA will be completed by the Project Lead and submitted to the Information Governance Department (IG) for Recommendations for approval by the Approval Group (see 4.2.20-21).

3.3. IG will maintain a log of all completed PIAs.

3.4. Copies of the PIAs will be used as evidence on the Data Security Standards (formerly known as IG Toolkit), as well as evidence in the

investigation of breaches of confidentiality or information security, and may be requested by the Information Commissioner's Office (ICO).

3.5. A PIA must identify and manage risks as part of good governance and good business practice. The end results of an effective PIA are:

- the identification of the project's privacy impacts;
- appreciation of those impacts from the perspectives of all stakeholders;
- an understanding of the acceptability of the project and its features by the Trust and third party, as well as the people that will be affected by it;
- consideration and assessment of less privacy invasive alternatives;
- identification of ways to lessen negative impacts on privacy;
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them.

4. Process

4.1. Identifying need for a PIA

4.1.1. A PIAs must be undertaken at the commencement of a project as detailed below:

- commence a PIA as part of the project initiation phase (or its equivalent in whichever project method the organisation uses) ensuring that project risks are identified and appreciated before the problems become embedded within the design; and
- if the project is already under way, start immediately, therefore any major issues are identified with the minimum possible delay.

4.1.2. The PIA template contains Screening Questions to assist in establishing the need for a PIA. This is a non-exhaustive list. (http://uhbpolicies/assets/PrivacyImpactAssessmentProcedureAppendixA.docx)

4.2. Completing a PIA

A template PIA is provided at:

http://uhbpolicies/assets/PrivacyImpactAssessmentProcedureAppendixA.docx. All sections must be completed using the guidance below.

4.2.1. *What does the project aim to achieve?*

- State the aim of the project, and what the PIA applies to. If there are different phases to a project, this section must make clear to which phase the PIA applies.

- Project documentation may be attached to the PIA, but this section must still contain an explanation of what project.

4.2.2. *What are the benefits to the organisation?*

This section must provide details of how the project will benefit the Trust. Reference may be made to Project documentation, but the main benefits must be listed.

4.2.3. *State the name of the Information Asset Owner and Information Asset Administrator and confirm that asset will be added to the register on completion*

- Details of the Information Asset Owner (IAO) and Administrator (IAA) must be included on the PIA and confirmation that it will be added to the Information Asset Register (IAR).

- All Information Assets (IA) must be included on the (IAR). Please refer to the associated IAR Procedure.

4.2.4. *What data will be collected?*

- A list of all the data fields that are to be captured must be provided. This list may be given in an appendix to the PIA or within the document itself.

- The Trust Informatics team must be contacted for further advice on meeting this requirement.

4.2.5. *How is the data collected?*

- This section must state the method by which data is to be collected.

- If the data is collected electronically from other systems, the PIA must state if the feed is manually received or automatic.

- If the data is collected electronically, the PIA must state how the information is inputted, such as manually, by a clinician or by a patient.

- If the data is collected on paper, the PIA must state how the information is inputted, such as manually, by a clinician or by a patient.

4.2.6. *What is the legal basis for the collection of this new information?*

- Under the Data Protection legislations, conditions for processing data by identifying a lawful basis must be established before processing of personal data.

- Lawful bases for processing personal and sensitive data including: Consent by data subject, performance of contract to which data subject is party; compliance with legal obligation; research; performance of a task carried out in the public interest; protection of vital interests of data subject.

- Further information about this can be obtained from the Information Commissioner's Office website, Information Governance can be consulted for any resulting queries.

4.2.7. *If consent is the legal basis for the use of the data, how is it obtained? Does the consent form require some positive, affirmative action? What information has been given to the data subject prior to consent being obtained? How has the consent by the data subject been recorded? Attach a copy of the consent form and any guidance leaflets where applicable.*

- If consent is required, this must be stated within the PIA and details as to the method of collection provided stating how it will be collected. Any consent forms or information leaflets must also be attached.

- If consent is not required, the legal basis for processing the data must be stated.

- For further guidance on Consent please refer to GDPR Guidance on Consent for Information Sharing Purposes.

4.2.8. *Is personal data of children being used? If so, has parental permission been obtained for the use of this information? Has the privacy notice been written in clear, plain language which a child can understand?*

- Children merit specific protection with regard to their personal data as considered as vulnerable individuals, therefore any information and communication where processing is addressed to a child, must be in language which is clear and plain in order that the child can easily understand it.

- Where online information services are provided for children and consent is relied on as the basis for the lawful processing, consent must be given or authorised by a person with parental responsibility for the child.

- The consent of the holder of parental responsibility may not be necessary in the context of preventive or counselling services offered directly to a child

4.2.9. *Has the data subject been informed about:*

- Purposes of the processing?

- Contact details of the data protection officer?

- Rights to access, withdraw, delete and/or rectify the data collected? (N.B. the right to 'delete' personal data does not apply to 'health data').

- How these rights can be exercised (email address/ telephone number)?

- When these rights can be exercised (i.e. following the applicable retention period?

- How to lodge a complaint?

- List/categories *of recipients of data?*

These are the minimum information that required by the Data Protection Regulations to be provided before personal data are collected from the data subject, i.e. patient information sheet or customised privacy notice.

4.2.10. *What checks have been made to ensure you are collecting the minimum amount of data necessary for the project?*

The 3rd Caldicott Principle provides that only the minimum amount of information necessary for the project is collected. An explanation must be given in the PIA detailing how the data set being collected has been agreed. This may include, but not

limited to approval by the Project Board or Working Group, or clinical input.

4.2.11. *Who will have access to the data, for what purpose and what access controls will be in place?*

- The PIA must clearly state which people will have access to the data, including any Trust or external IT support staff.

- If there are different levels of access, these must be clearly stated and define who has access to what at which level. For example a table could be provided:

Level of Access	Information Accessible	Job Role / Name

- Details of how access is granted, reviewed and removed must be clearly stated in the PIA. A named person (Manager) must take responsibility for this. http://uhbpolicies/assets/PrivacyImpactAssessmentProcedureAppendixB.docx may be used to grant access to the system.

- Details of the authentication process for accessing the data must be provided in the PIA. This may include details of password security, strength and the frequency of password resets.

- If the data is accessible or inputted on an external-facing system, details of access process for external users must be provided.

4.2.12. *What audit system is in place to assess who has accessed the data?*

- Access to data must be subject to an audit in accordance with national NHS standards.

- The PIA must explain how activity will be audited and may also be used to provide evidence to support investigations into suspected or actual breaches in patient confidentiality, data security, fraud and/or corruption.

4.2.13.*How have the information security risks been assessed?*

- The PIA must address how the information security risks have been assessed, what processes have been used to mitigate the risks and how compliance will be monitored.

- As a minimum the following areas must be covered:

  a) technical security
  b) physical security
  c) data recovery/business continuity
  d) encryption facilities
  e) network security management
  f) penetration tests for external-facing systems
  g) emergency access
  h) malware protection/detection
  i) privacy and security monitoring and reporting function
  j) security incident response plan
  k) user education & training
  l) health data integrity and authenticity
  m) cyber security product upgrades for 3rd party systems

- The Trust Information Security team must be contacted for further advice on meeting this requirement.

4.2.14. *Will any data be transferred outside the UK?*

- If data is being transferred outside the UK, details of the recipient country must be stated.

- The method of transmission must also be described.

4.2.15.*How will the data be kept up-to-date and accurate?*

- The 4th principle of the Data Protection Act and the GDPR requires data to be kept up-to date and accurate. The PIA must explain how the data being collected meets this requirement.

- This explanation may also include details of the training users of the system or those who input data will receive.

- If the data is collected via manual or automatic electronic feeds, details of the frequency and method must be provided.

4.2.16. *What action is being taken to ensure the quality of the data?*

- Details of how the quality of the data is assessed must be provided. This may take the form of audits of the data inputted.

- The frequency and size of such audits will be dependent on the purpose for the data collection.

4.2.17. *How long will the data be retained for?*

The data will need to be kept in accordance with the NHS Records Management Code of Practice. Justification must be given if the data is to be kept contrary to this.

4.2.18. *Consultation Requirements*

If consultation is necessary for the project, details of this must be provided.

4.2.19. *Information Risk Assessment*

- A full Information Risk Assessment must be carried out. The Trust Risk Assessment template (http://uhbhome/risk-assessment-documents.htm) may be used (. All sections must be completed in accordance with the Trust Risk Matrix (http://uhbpolicies/assets/RiskRegistersAssessmentManagementProcedure.pdf).

- The 'risk significance' score is to be based on the situation following the risk mitigation.

- Any controls/actions and people responsible must be identified.

4.2.20. *Recommendations by IG*

This section will be completed by the IG. The recommendations will incorporate any advice from IT Security and Informatics and will take into account any risks and actions to be completed.

4.2.21. *Digital Healthcare Group (DHG) /Information Governance Group (IGG) Approval*

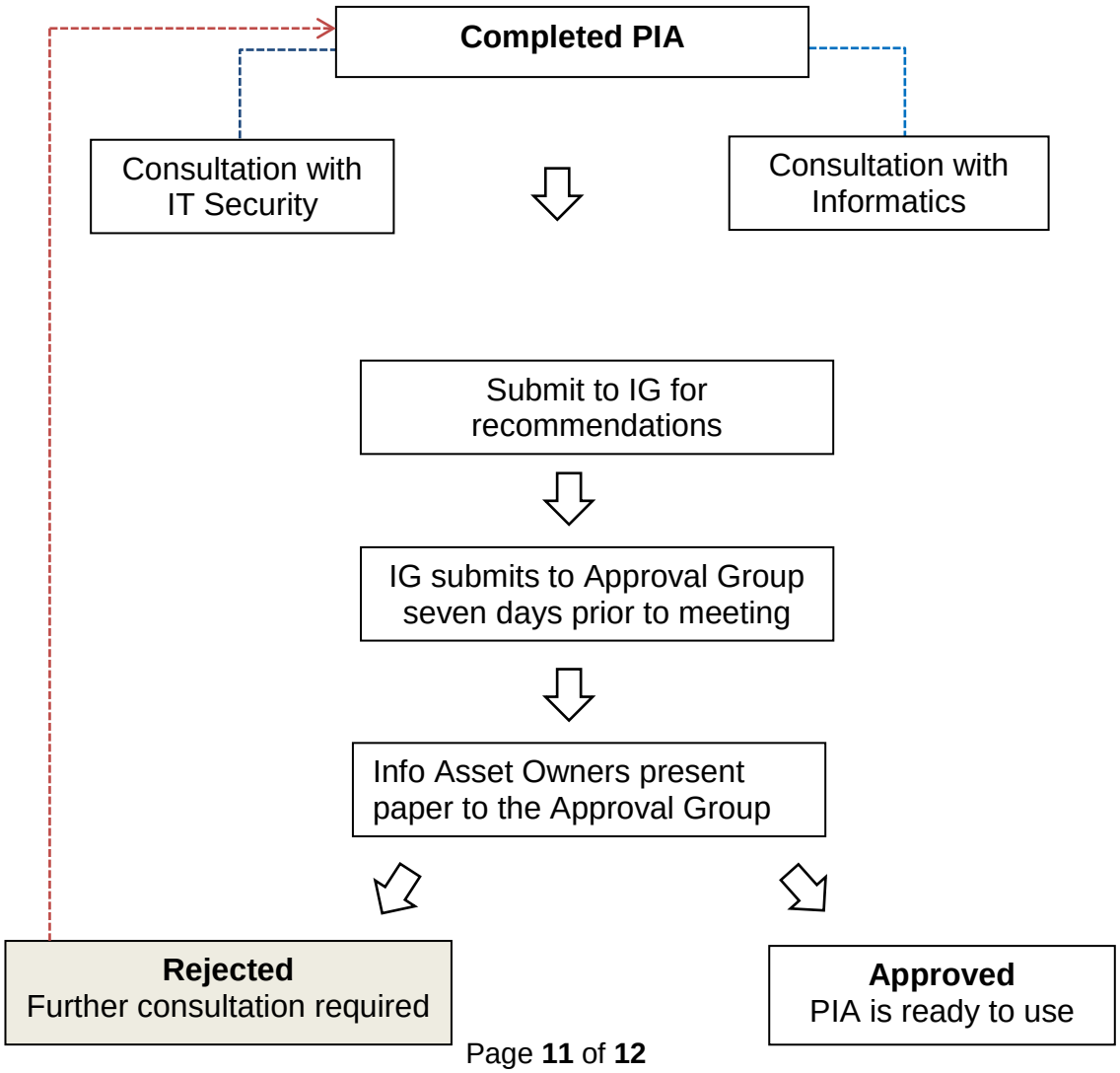
- PIAs must be approved by the following:

Type of data	Approval Groups
Patient information	DHG
Staff Information	IGG
Staff and Patient Information	DHG
Other Information	IGG

- PIAs must only be approved outside of these approval groups in exceptional circumstances and with the permission of either the Trust's Senior Information Risk Owner (SIRO) or Caldicott Guardian.

- PIAs must be submitted to the IG in order for an IG recommendation to be made. The IG will submit the PIA to the Chair of the approval groups seven days prior to the meeting where approval will be sought, unless exceptional circumstances apply.

- The approval process as described on the following diagram:



5. References

Caldicott Principles

Data Protection Act 1998 and 2018 (subject to Royal Ascent)

The General Data Protection Regulation (EU) 2016/679

ICO Conducting Privacy Impact Assessments Code of Practice

NHS Records Management Code of Practice

6. Associated policy and procedural documentation

Data Protection and Confidentiality Policy

GDPR Guidance on Consent for Information Sharing Purposes

IT Acceptable Use Policy

Information Asset Register Procedure

Information Governance Policy

Information Security Policy

Procedure for the Assessment of Risks and Management of Risk Registers