PRIVACY IMPACT ASSESSMENTS (PIA)

A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, a declaration of incompatibility with the Human Rights Act, or prohibitive costs in retro-fitting a system to ensure legal compliance or address concerns about privacy.

- It is the personal responsibility of every individual referring to this policy to ensure that they are viewing the latest version; this will always be published on Cygnet's SharePoint.

INDEX

1. INTRODUCTION

This guidance and template is a practical tool to help identify and address the data protection and privacy concerns at the design and development stage of a project, building data protection compliance in from the outset rather than bolting it on as an afterthought. This document details the process for conducting a Privacy Impact Assessment (PIA) through a project lifecycle to ensure that, where necessary, personal and sensitive information requirements are complied with and risks are identified and mitigated.

A PIA should be carried out whenever there is a change that is likely to involve a new use or significant change in the way personal data is handled, for example a redesign of an existing process or service, or a new process or information asset is being introduced.

Completion of a PIA should be built into the organisational business approval and procurement processes.

This procedure is to be considered in the following circumstances:

- Introduction of a new paper or electronic information system to collect and hold personal data.
- Update or revision of a key system that might alter the way in which the organisation uses, monitors and reports personal information.
- Changes to an existing system where additional personal data will be collected.
- Proposal to collect personal data from a new source or for a new activity.
- Plans to outsource business processes involving storing and processing personal data.
- Plans to transfer services from one provider to another that include the transfer of information assets.
- Any change to or introduction of new data sharing agreements.

This list is not exhaustive.

Any systems which do not identify individuals in any way do not require a PIA to be performed. However, it is important to understand that what may appear to be "anonymised" data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that it will not identify individuals.

The Corporate Information Governance Manager will advise any services regarding whether a PIA needs to be completed and support them with review of the PIA template. To contact the Information Governance Manger please email: dataprotection@cygnethealth.co.uk

There is a statutory requirement under the General Data Protection Regulation (GDPR) to complete a Privacy Impact Assessment at the start of a project.

NHS Digital have included PIAs as a standard in the Data Protection and Security Toolkit. This template is based on the Information Commissioners Office guidance on implementation and use of PIAs and has been adapted for use within health settings. The CQC also assess Information Management as part of the 2018/2019 Key Lines of Enquiry (KLOE).

2. WHO IS RESPONSIBLE FOR COMPLETING A PIA?

Any person who is responsible for introducing a new or revised service or changes to a new system process or information asset is the Information Asset Owner (IAO) and is responsible for ensuring the completion of a PIA. However a PIA can be completed by the Business Systems Team or the Corporate Information Governance Manager if appropriate.

The Corporate Information Governance Manger should be consulted at the start of the design phase of any new service, process, purchase of or implementation of an

information asset1, so that they can advise on the need and procedures for completing the PIA.

These would then be reported back to the Information Governance Board where significant issues could be raised with the Caldicott Guardian and Senior Information Risk Owner in order for a further risk assessment to be performed if appropriate to do so.

2.1 The role of the Information Asset Owner: a practical guide (Extracts)

Information Asset Owner (IAO) is a mandated role and the individual appointed is responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

An Information Asset Owner is appointed by the Senior Information Risk Owner (SIRO), who in turn reports to the Chief Operating Officer.

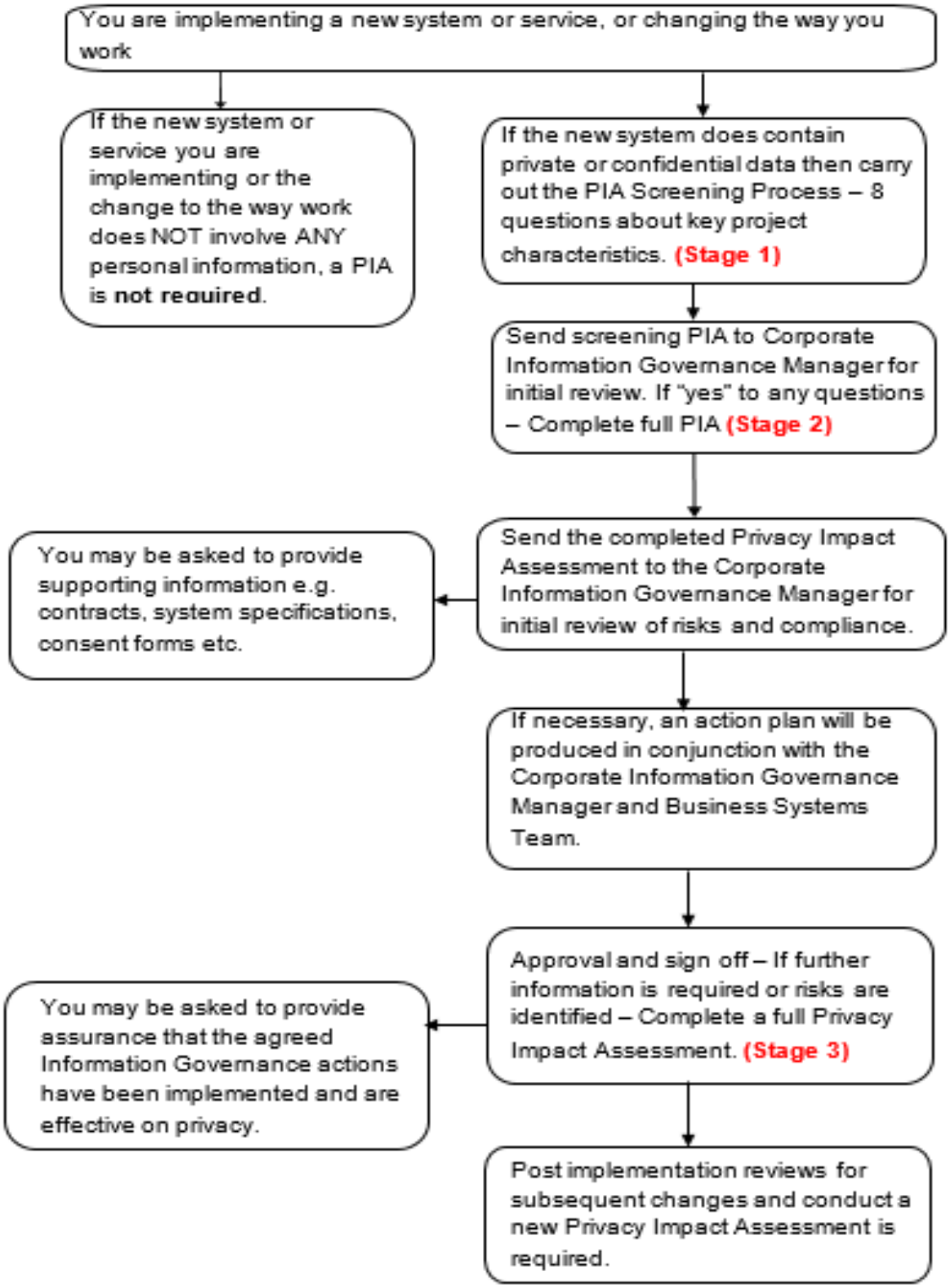
"Performing the role well brings significant benefits. It provides a common, consistent and unambiguous understanding of what information you hold, how important it is, how sensitive it is, how accurate it is, how reliant you are on it, and who's responsible for it. It helps ensure that you can use the information you need to operate transparently and accountably, for example to meet data standards, to unlock previously unavailable data and to improve services."

The full document the above extracts are taken from can be found at:
http://www.nationalarchives.gov.uk/documents/information-management/role-of-the-iao.pdf

The IAO may appoint Information Asset Administrator/s (IAAs) as their deputies and/or to carry out the day to day management and operation of their information asset. Please note the Business Systems Team will be classed as IAAs for all assets as they manage the information assets on behalf of the business.

[1] An Information Asset can be Operating systems, infrastructure, business applications, off-the-shelf products, services, user developed applications, records and information.

3. PRIVACY IMPACT ASSESSMENT FLOWCHART



4. THREE STAGES OF A PIA

Please complete an overview of the project first using Appendix 1. This should be the front sheet for all assessments that follow.

4.1 Stage 1 - The initial screening questions (Appendix 2)

This section is to be completed by the Information Asset Owner or project lead responsible for delivering the proposed change.

The purpose of the screening questions is to check whether a further PIA assessment is required and to ensure that the investment in the organisation is proportionate to the risks involved. If the response to any of the questions is "yes" then an initial Privacy Impact Assessment should be completed.

A meeting with the Corporate Information Governance Manager should be arranged to review the responses and discuss whether a stage 2 assessment should be completed.

4.2 Stage 2 – Privacy Impact Assessment (Appendix 3)

The responses to the screening questions will give an indication as to the appropriate scale of the PIA. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

This should be completed by the Information Asset Owner or project lead responsible for delivering the proposed change. The completed form will be assessed by the Corporate Information Governance Manager who will advise on the next stage.

4.3 Compliance checklist

The Privacy Impact Assessment also contains a data mapping template (Appendix 4) and data protection and privacy law compliance checks (Appendix 5) which need to be considered by the Data Protection Officer.

4.4 Stage 3 - Sign off forms and agreed actions (Appendix 6)

All PIAs should be signed off. Where the PIA identifies further Information Governance issues, an action plan should be developed on how the risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities and timescales and will be written in conjunction with the Corporate Information Governance Manager and Business Systems Manager ready for discussion at the Information Governance Board.

5. SUPPORTING GUIDANCE FOR COMPLETION OF THE PRIVACY IMPACT ASSESSMENT

1	**Information Asset** E.g. Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, devices/equipment, medical records and staff records.
2.	**Person Identifiable Data** Key identifiable information includes: name, address, full post code, date of birth; pictures, photographs, videos, audio-tapes or other images of people; NHS number, NI number and other local identifiable codes; Anything else that may be used to identify persons directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
3.	**New use of information could include:** Data Extracts involving new fields of patient confidential data Setting up a database or independent Service User System Introducing a new HR system Reports **Examples of changes to use of information could include:** Moving paper files to electronic systems Collecting more data than before Using Data Extracts for a different purpose Additional organisations involved in information process Revisions to systems, databases (including mergers)
4.	**Data Flow Mapping and the Data Inventory** A Data Flow Map is a graphical representation of the data flow. This should include: Incoming and outgoing data Organisations and/or people sending/receiving information Storage for the 'Data at Rest' i.e. system, filing cabinet Methods of transfer
5.	**Examples of additional documentation which may be required (copies):** Contracts, Confidentiality Agreements, Project Specification, Consent Forms, System Specifications (including access controls), Local Access Controls Applications, and Information provided to Service Users and Staff.

REFERENCES

Privacy Impact Assessments – The Information Commissioners Office
http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx.
Information Governance Toolkit – NHS Digital
https://www.igt.hscic.gov.uk/
General Data Protection Regulation – Council of the European Union
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

APPENDIX 1

Privacy Impact Assessment – project details

This Privacy Impact Assessment must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled.

PIA reference number:	**To be provided by the Business System Team**		
Project description:			
Date assessment completed:			
Implementing site/department:			
Project Manager details: **Name:** **Role:** **Contact details:**			
Overview: **(summary of the proposal)** **What the project aims to achieve**			
Proposed implementation date:			
State the purpose of the project – e.g. patient treatment, administration, audit, research etc.			
Key stakeholders (including contact details) – can include – project management team, developers, data processors, designers	Name	Job title	Contact number

APPENDIX 2

Stage 1 – Initial screening questions

Answering "Yes" to any of the screening questions below represents a potential Information Governance risk factor that will have to be further analysed to ensure those risks are identified, assessed and fully mitigated.

Q	Screening question	Yes/No
1.0	Will the project/process include the processing of personal or confidential data?	
1.1	Will the project involve the collection of new information about individuals?	
1.2	Will the project compel individuals to provide information about themselves?	
1.3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
1.4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
1.5	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	
1.6	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	
1.7	Is the information about individuals likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private?	
1.8	Will the project require you to contact individuals in ways which they may find intrusive?	
1.9	Has this project/process already been started as a pilot without a PIA being undertaken?	

If you have answered "Yes" to any of the questions below please proceed and complete stage 2. Email the Data Protection Officer and request a meeting to review the completed documents: dataprotection@cygnethealth.co.uk

APPENDIX 3

Stage 2 – Privacy Impact Assessment

2.1	**Is this a new or changed use of personal information that is already collected?**	**New/Changed**
2.2	**What data will be collected?**	
	Administration data Forename: Surname: DoB: Age: Gender: Address: Postcode: NHS No: NI No: Payroll No: Any other unique identifier (please specify) : Other data (please state): **Sensitive data** Racial or ethnic origin Political opinion Religious belief Trade Union membership Physical or mental health or condition Sexual life Commission or alleged commission of an offence Proceedings for any offence committed or alleged Will the dataset include clinical data? Yes/No Will the dataset include financial data? Yes/No **Description of other data collected** **Is the information being used for a different purpose than it was originally collected for?**	

<table>
<tr><td rowspan="6">2.3</td><td colspan="2">Are other organisations involved in processing the data?</td><td colspan="2">Yes/No
If yes, list below</td></tr>
<tr><td>Name of Organisation</td><td>Data Controller (DC) or Data Processor (DP)?</td><td colspan="2">Completed and compliant with the IG Toolkit</td></tr>
<tr><td></td><td></td><td>Complete Y/N</td><td>Overall Rating</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>2.4.</td><td colspan="2">Has a data flow mapping exercise been undertaken? If yes, please provide a copy- template attached, if no, please undertake – see page 13 for guidance</td><td colspan="2">Yes/No</td></tr>
<tr><td>2.5</td><td colspan="2">Does the work involve employing contractors external to the organisation?
If yes, provide a copy of the confidentiality agreement or contract?</td><td colspan="2">Yes / No</td></tr>
<tr><td>2.6</td><td colspan="4">Describe in as much detail why this information is being collected/used?</td></tr>
<tr><td>2.7</td><td colspan="2">Will the information be collected electronically, on paper or both?</td><td colspan="2">Electronic □
Paper □</td></tr>
<tr><td>2.8</td><td colspan="4">Where will the information will be stored:</td></tr>
<tr><td>2.9</td><td colspan="2">Will this information being shared outside the organisations listed above in question 2.3?
If yes, describe who and why:</td><td colspan="2">Yes/No</td></tr>
<tr><td>2.10</td><td colspan="2">Is there an ability to audit access to the information?</td><td colspan="2">Yes/No</td></tr>
<tr><td>2.11</td><td colspan="4">Does the system involve new links with personal data held in other systems or have existing links been significantly changed?</td></tr>
</table>

2.12	**How will the information be kept up to date and checked for accuracy and completeness (data quality)? If you are procuring new software does it allow you to amend data when necessary? How are you ensuring that personal data obtained from individuals or other organisation is accurate?**		
2.13	**Who will have access to the information?** (list individuals or staff groups)		
2.14	**What security and audit measures have been implemented to secure access to and limit use of personal identifiable information?** Username and password ☐ Key to locked filing cabinet/room ☐ Restricted access to network files ☐ Other: Provide a description below:		
2.15	**Will any information be sent offsite – i.e. outside of the organisation and its computer network** Are you transferring personal data to a country or territory outside of the EEA?		
2.16	**Please state by which method the information will be transferred?** Email (not NHS.net) ☐ Fax ☐ Nhs.net email ☐ Courier ☐ Website access ☐ Post (internal) ☐ Post (external) ☐ By hand ☐ Telephone ☐ Wireless network ☐ Other: (please specify)		
2.17	**Are disaster recovery and contingency plans in place?**	Yes/No	
2.18	**Is Mandatory Staff Training in place for the following?** Use of the System or Service: Collecting Consent: Information Governance:	 Yes/No Yes/No Yes/No	Dates

2.19	**Are there any new or additional reporting requirements for this project?**	Yes/ No
	Who will be able to run reports? Who will receive the report or where will it be published? Will the reports be in person-identifiable, pseudonymised or anonymised format?	
2.20	**If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of? What retention periods are suitable for the personal data being processed? If software is being procured will information be deleted in line with the retention period?**	Yes/No
2.21	**How will individuals be informed about the proposed uses of their personal data?** (e.g. privacy notices)	
2.22	**Are arrangements in place for recognising and responding to patients requests for access to their personal data?**	Yes/No
2.23	**Will patients be asked for consent for their information to be collected and/or shared?** If no, list the reason for not gaining consent e.g. relying on an existing agreement or consent is implied: How will you manage service user wishes to withdraw consent?	Yes/No

Attachments may include:
For example confidentiality contracts, information security documentation, data protection and security toolkit scores, project implementation plan.

APPENDIX 4

Data mapping template

Please complete the following data mapping exercise:

This data mapping should be completed by filling in the details below. (Email Data Protection Officer for copies of spreadsheet with examples – dataprotection@cygnethealth.co.uk)

Identify what data is being processed – brief outline of why.	
Actual type of processing taking place.	
Identify/describe each item of personal data to be processed	
Purpose of processing	
Data Formats	
Which system is the data captured in? (If it is a paper file please write paper and how it is secured) If it is held on a shared drive give brief file pathway	
Who has access to the data? How do they access the data?	

Please ensure that all information is passed on to the Corporate Information Governance Manager to enter into the Data Inventory. You can do this by emailing dataprotection@cygnethealth.co.uk

Data Fields Table
Please complete the table below to show what fields will actually be collected.

Name of Field	What is the source of the data? Which system is it from?	Justification for use Explain why this field is required and how the project would be affected if not available.

APPENDIX 5

Privacy Impact Assessment – assessment of legal compliance

To be completed by the Data Protection Officer
Does the PIA meet the following legal requirements?
European General Data Protection Regulation 2018

Principle	Assessment of Compliance
Principle 1 – Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')	
Principle 2 – Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')	
Principle 3 – Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed ('data minimisation')	
Principle 4 – Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')	
Principle 5 – Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate	

technical and organisational measures required by this regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')	
Principle 6 – Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')	

Common Law Duty of Confidentiality

	Assessment of Compliance
Is there an appropriate method for collecting consent?	
Is the disclosure in the overriding public interest?	
Is there a legal duty to do so, for example a court order	
Is there a statutory basis that permits disclosure such as approval under Section 251 of the NHS Act 2006	

Human Rights Act 1998
The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Will your actions interfere with the right to privacy under Article 8? – have you identified the social need and aims of the project? **Are your actions a proportionate response to the social need?**

APPENDIX 6

Sign off forms and agreed actions

Identified risks, agreed actions and sign off form

What are the key privacy issues and associated compliance and corporate risks? (Some Privacy Issues may have more than one type of risk i.e. it may be a risk to individuals and a corporate risk)

Privacy issue	Risk to individuals	Compliance risk	Corporate risk

Describe the actions you could take to reduce the risk and any future steps which would be necessary (e.g. new guidance)

Risk	Solution(s)	Result: Is the risk reduced, eliminated or accepted?	Evaluation: Is the final impact on the individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

What solutions need to be implemented?

Risk	Approved solution	Solution approved by

Actions

Action to be taken	Date for completion	Responsibility for action

Have any other risks been identified which do not relate to Privacy but need to be escalated e.g. Business Continuity, Health & Safety?

Risk	Escalated to?

Sign Off

Information Governance/Data Protection Representative	
Name	
Job title	
Signature	
Date	

Business Systems Representative	
Name	
Job title	
Signature	
Date	

Caldicott/SIRO/CEO	
Name	
Job title	
Signature	
Date	

Lead/Project Manager	
Name	
Job title	
Signature	
Date	