Nene Clinical Commissioning Group

Data Protection Impact Assessment Procedure

Procedure Number: **IG07**

Version:	3..1
Approved by:	Information Governance Working Group
Date approved	January 2018
Ratified by:	Audit and Risk Committee
Date ratified:	February 2018
Name of originator/author:	Louise Chatwyn – Information Manager
Name of responsible individual:	Clare Hodgson – Deputy Director of Corporate Affairs
Review date:	May 2018
Target audience:	All Staff

Version Control Sheet

Version	Date	Who	Change
0.1	05/13		To GEM IG leads for comments
0.3	05/13		Final draft for approval
0.4	07/13		Minor changes in text with information lead at CCG
0.6	07/13		Reviewed in line with ICO guidance
1.0	09/13		Approved at Information Governance Committee
1.1	06/14		Reviewed in line with ICO guidance
			Review for CCG ownership
1.3	06/14		Amended in line with comments from GEM product group
2.0	08/14		Approved at Information Governance Product Group
3.0	06/16	L Chatwyn	Review and update to current
3.1	07/17	L Chatwyn	Minor revisions to reflect current legislation and practice and changes under the General Data Protection Regulations (GDPR)

Contents

1. Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

A Data Protection Impact Assessment (DPIA) should be carried out whenever there is a change that is likely to involve a new use; or significantly change the way in which 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 DPIA should be built into the organisational business approval and procurement processes.

This document 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. It sets out Nene CCGs procedure for conducting a (DPIA) through a project lifecycle to ensure that, where necessary, personal and sensitive information requirements are complied with and risks are identified and mitigated

2. Purpose

There is currently no statutory requirement for any organisation to complete a PIA. However, central Government departments have been instructed to complete PIAs by Cabinet Office and the Department of Health has included PIAs as a standard in the Information Governance 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

Under the General Data Protection Regulation (GDPR) which will come into effect in May 2018 this will become an express legal requirement

This document is a statement of the approach and intentions for Nene CCG to fulfil its statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

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

3. Scope

This document applies to all staff, whether permanent, temporary or contracted. They are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis.

Furthermore, the principles of this document apply to all third parties and others authorised to undertake work on behalf of Nene CCG.

This document covers all aspects of information, in both paper and electronic format

4. Key Roles and Responsibilities

Role	Responsibility
Accountable Officer	The Accountable Officer and the Board have ultimate accountability for actions and inactions in relation to this document
Senior Information Risk Officer	The CCGs SIRO is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality function. The role includes briefing the Board and providing assurance through the Audit and Risk Committee that the IG approach is effective in terms of resource, commitment and execution. The SIRO for Nene CCG is the Chief Finance Officer
Caldicott Guardian	The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles. The Caldicott Guardian for Nene CCG is the GP Chair
Data Protection Officer	The DPO has responsibility for Data Protection compliance The DPO role for Nene CCG is fulfilled by NEL CSU

Deputy Director of Corporate Affairs	The Deputy Director of Corporate Affairs has overall day to day responsibility for the Information Governance in the CCG. The role includes briefing the Board, including the SIRO and Caldicott Guardian of information risks and information incidents
Information Manager	The Information Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation The Information Manager is responsible for overseeing completed data protection impact assessments and advising on identified risks and mitigations
Managers	Managers and supervisors are responsible for ensuring that staff who report to them have suitable access to this document and it's supporting policies and procedures and that they are implemented in their area of authority. Managers are also responsible for ensuring the initial training compliance of all staff reporting to them
All staff	Have a responsibility to: • Be aware of the Information Governance requirements • Support the CCG to achieve Toolkit Compliance • Complete annual IG training • Report information Incidents appropriately

5. Process

Any systems which do not identify individuals in any way do not require a DPIA 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.

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 DPIA. This is usually the project manager.

A Two Tier approach to the agreement and approval of Information Sharing will be adopted as follows:

- Tier One will capture the rules, laws, principles and standards that have been adopted by all partner organisations within the Local Digital Roadmap.
- Tier Two will consist of the templates and documents resulting from them, that cover Information Sharing Protocols and Data Protection Impact Assessments

The Data Protection Impact Assessment template can be found at Appendix 1

5.1 Full scale Data Protection Impact Assessment

In most small scale projects the DPIA may identify one or more IG risks and the lead manager will be advised on the actions necessary to mitigate or eliminate those risks.

Where the DPIA discovers complex or several IG risks, an action plan should be developed on how the risks will be mitigated a report should be produced. The final report should cover (where applicable):

- A description of the proposal including the data flow process
- The case justifying the need to process an individual's personal data and why the particular policy or project is important
- An analysis of the data protection issues arising from the project
- Details of the parties involved
- Details of the issues and concerns raised
- Discussions of any alternatives considered to meet those concerns, the consultation process, and the rationale for the decisions made
- A description of the privacy by design features adopted
- An analysis of the public interest of the scheme
- Compliance with the data protection principles
- Compliance with the Government Data Handling review's information security recommendations
- Where the proposal involves the transfer and storage of personal data the PIA should include details of any security measures that will be put into place to ensure the data is protected and kept secure.

The organisations Caldicott Guardian and/or Senior Information Risk Owner (SIRO) should be included at an early stage to ensure adequate consultation of the DPIA.

6. Monitoring and Review

Performance against key performance indicators will be reviewed on an annual basis through the IG Toolkit submission and used to inform the development of future documents.

Unless there is major legislation or policy, this document will be reviewed annually

7. Training

Appropriate Information Governance training will be provided to all staff annually.

Training is available through ESR which can be found here:
http://www.esrsupport.co.uk/access.php

8. Distribution and Implementation

All policy and procedural documents in respect of Information Governance will be made available via the Nene CCG staff intranet.

Staff will be made aware of procedural updates as they occur via team briefs, management communications and notification via the CCG staff intranet.

9. Associated Legislation and Documents

To include but not limited to:

- Information Governance Policy and Management Framework
- Information Governance Incidents Cyber Security Incidents and Near Misses Reporting Procedure
- Confidentiality Data Protection Policy
- Information Security Policy
- Information Asset Management Procedure
- Information Disclosure and Sharing Policy and Procedure

The following references and areas of legislation should be adhered to.

- Confidentiality NHS Code of Practice
- Data Protection Act 1998
- Caldicott Guardian principles
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records 1990
- Records Management NHS Code of Practice
- General Data Protection Regulation (GDPR)

10. References

Information Commissioner's Office PIA Code of Practice
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

The IG Toolkit
https://nww.igt.hscic.gov.uk/

Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

EU General Data Protection Regulation (GDPR)
https://www.eugdpr.org/

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation
https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf

The NHS Constitution for England
https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england

NHS Code of Confidentiality
https://www.england.nhs.uk/wp-content/uploads/2013/06/conf-policy-1.pdf

NHS Care Record Guarantee
http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf

NHS Information Risk Management
http://systems.hscic.gov.uk/infogov/security/risk

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents

11. Appendices

Appendix 1 The Data Protection Impact Assessment

A word copy of the assessment document is available from the Information Team

Northamptonshire Digital Roadmap

December 2017

Data Protection Impact Assessment Template

Data Protection Impact Assessment (DPIA)

Project description	
Implementing organisation	
Project Manager details: **Name** **Designation** **Contact details**	
Implementation date	

Data Protection impact assessment screening questions

Answering 'yes' to any of these questions is an indication that a DPIA is a necessary exercise. You can expand on your answers as the project develops if you need to. You can adapt these questions if necessary for unusual circumstances.

Questions	Yes/No
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	
Will the project require you to contact individuals in ways which they may find intrusive?	

Step one: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the DPIA process.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Privacy Issues	Risks to individuals	Compliance Risks	Associated/ Corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

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

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Action to be taken	Date for completed actions	Responsibility for action

Contact point for future privacy concerns:

Appendix 2 Data Mapping Data Mapping

As part of the DPIA process we should describe how information is collected, stored, used and deleted. We should explain what information is used, what it is used for and who will have access to it.

A thorough assessment of privacy risks is only possible if an organisation fully understands how information is being used in a project. An incomplete understanding of how information is used can be a significant privacy risk – for example; data might be used for unfair purposes, or disclosed inappropriately.

This part of the DPIA process can be integrated with any similar exercises which would already be done for example; we already conduct information audits, develop information maps, and make use of information asset registers.

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

If such data has already been captured covering the proposed project or similar document this can be useful for understanding how personal data might be used.

The information flows can be recorded as a flowchart, an information asset register, or a project design brief which can then be used as an important part of the final DPIA report.

Describing information flows

- Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.
- This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing)
- People who will be using the information are consulted on the practical implications.
- Potential future uses of information are identified, even if they are not immediately necessary.