***WILLINGHAM MEDICAL PRACTICE***

& LONGSTANTON BRANCH SURGERY

**Data Protection Impact Assessment (DPIA)**

**Data Protection Impact Assessment (DPIA)**

**TEMPLATE**

**Version Control Sheet**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date Issued** | **Details**  |

|  |
| --- |
| **Brief Summary of Change**  |

 | **Author** |
| 1.0 |  03.03.2020  |  | New document | Lisa Smith |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| **For more information on the status of this policy, please contact:**  |
| Willingham Medical Practice  | Governance Board  |
| Approved by | Board |
| Approval Date |  |
| Next Review Date |  |
| Responsibility for Review | Information Governance Team |
| Contributors | IG Lead, SIRO, Caldicott Guardian |
| Audience | All officers and staff (which includes temporary staff, contractors and seconded staff). |

**Data Protection Impact
Assessment**

|  |  |
| --- | --- |
| What is the name of the project, system or process that this DPIA document relates to? |  |
| Key contact name: |  |
| Key contact details – email, landline and mobile |  |

This questionnaire is a mandatory document requiring completion as part of a project, whether it is procuring and implementing a new system or a change in business process for example, to identify any impact on the handling of personal confidential data (PCD) irrespective of whom it relates to, e.g. service users, staff, customers or third party contractors.

Table of Contents

[1. Introduction 5](#_Toc12534135)

[2. Purpose 5](#_Toc12534136)

[3. Scope 6](#_Toc12534137)

[4. Key Roles and Responsibilities 6](#_Toc12534138)

[5. Process 7](#_Toc12534139)

[6. Full scale Data Protection Impact Assessment 7](#_Toc12534140)

[7. Monitoring and Review 8](#_Toc12534141)

[8. Associated Legislation and Documents 8](#_Toc12534142)

[9. References 9](#_Toc12534143)

[10. Data Protection Impact Assessment 10](#_Toc12534144)

[10.1. Section One 10](#_Toc12534145)

[10.2. Section Two 11](#_Toc12534146)

[10.3. Section Three 12](#_Toc12534147)

[10.4. Section Four 18](#_Toc12534148)

[10.5. Section Five - Risk– To be completed by the IG Team Only 22](#_Toc12534149)

[10.6. Section Six – DPA 2018 / GDPR – To be completed by the IG Team Only 22](#_Toc12534150)

[10.7. Section Seven – Caldicott – To be completed by the IG Team Only 23](#_Toc12534151)

[10.8. Statement of Assessment 24](#_Toc12534152)

# 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 Willingham Medical Practice 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.

# 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 Willingham Medical Practice 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

# 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 Willingham Medical Practice

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

# 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 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 Willingham Medical Practice is the Practice Manager |
| **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 Willingham Medical Practice is Dr Jankovic.  |
| **Data Protection Officer**  | The DPO has responsibility for Data Protection compliance The DPO role for Willingham Medical Practice is the CCG.  |
| **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 Willingham Medical Practice to achieve Toolkit Compliance
* Complete annual IG training
* Report information Incidents appropriately
 |

# 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

# 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.

# 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.

# 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)

# 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>

# Appendix 1 - Data Protection Impact Assessment Check Sheet

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?  |  |

# Appendix 2 - Data Protection Impact Assessment

# Section One

Please complete with as much information as possible as this will assist in assessing whether further action is required.

|  |  |
| --- | --- |
| **Information Asset/Project Name** |   |
| **Directorate/Department** |   |
| **Organisation** |  |
| **Is this a change to an existing process?** |   |
| **Assessment Completed By** | Name:Title:Dept:Landline:Mobile:Email: |
| **Date completed** |  |
| **Information Asset Owner(s)**The senior person(s) responsible for the system – Director or AD level | Name:Title:Dept:Landline:Mobile:Email: |
| **Information Asset Administrator(s)**Usually a manager or super user of the system. Reports to and supports the IAO | Name:Title:Dept:Landline:Mobile:Email: |
| **Project/Change Outline - What is it that is being planned?** If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required. |
|  |
| **Purpose / Objectives - Why is it being undertaken?** This could be the objective of the process or the purpose of the system being implemented as part of the project. |
|  |
| **What is the purpose of collecting the information within the system?** For example patient treatment, patient administration, research, audit, reporting, staff administration etc. |
|  |
| **What are the potential privacy impacts of this proposal - how will this change impact upon the data subject?** Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing. |
|  |
| **Provide details of any previous Privacy / Data Protection Impact Assessment or other form of personal data compliance assessment done on this initiative.** If this is a change to an existing system, a DPIA may have been undertaken during the project implementation  |
|  |

# Section Two

In order to understand the potential privacy risks, it is important to know the types of data that is held and/or shared.

|  |  |  |  |
| --- | --- | --- | --- |
| Personal  | Please Tick All that Apply | Sensitive | Please Tick All that Apply |
| Name  | [ ]  | Racial / ethnic origin  | [ ]  |
| Address (home or business)  | [ ]  | Political opinions  | [ ]  |
| Postcode  | [ ]  | Religious beliefs  | [ ]  |
| NHS No  | [ ]  | Trade union membership  | [ ]  |
| Email address  | [ ]  | Physical or mental health  | [ ]  |
| Date of birth  | [ ]  | Sexual life  | [ ]  |
| Payroll number  | [ ]  | Criminal offences  | [ ]  |
| Driving Licence [shows date of birth and first part of surname]  | [ ]  | Biometrics; DNA profile, fingerprints  | [ ]  |
|  |  | Bank, financial or credit card details  | [ ]  |
|  |  | Mother’s maiden name  | [ ]  |
|  |  | National Insurance number  | [ ]  |
|  |  | Tax, benefit or pension Records | [ ]  |
|  |  | Health, adoption, employment, school, Social Services, housing records | [ ]  |
|  |  | Child Protection | [ ]  |
|  |  | Safeguarding Adults | [ ]  |
| Additional data types (if relevant) |  |
|  |
|  |
|  |

# Section Three

Please answer the questions below as fully as possible. If you are unsure of how to answer the question, please contact the relevant IG Team. If there is supporting information that relates to any of the questions, which you feel would be informative, indicate within the comments section and send this along with the completed assessment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment Questions** | **Yes/No** | **Comments** | **Risk Score** | **Outcome** |
| 1. Is it likely that the project will involve processes that are subject to DH guidance/legislation/Caldicott principles/Medical Record Standards? (if you are unsure, please look at the list below, as examples of what process types would be included).
 |   |  |  |  |
| If you have answered ‘Yes’ to the above, please indicate (with an X) if the following activities are included within the project:Recording of Demographic dataSharing of Patient informationDiagnostic activity resultsReporting of patient activityTransfer of Patient Identifiable Data to other systems, Patient, GP or other Third parties.Other (Please State) | [ ] [ ] [ ] [ ] [ ] [ ]  |  |  |  |

| **Category** |  | **Yes/No** | **Comments** | **Risk Score** | **Outcome** |
| --- | --- | --- | --- | --- | --- |
| Technology | 1. Does the project involve new or inherently privacy-invasive technologies e.g. biometrics or facial recognition?
 |   |  |  |  |
| *In order to answer this question, considerations include: - whether all of the information technologies that are to be applied in the project are already well-understood by the public; - whether their privacy impacts are all well-understood by the organisation, and by the public; - whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected; and* *- whether all of those measures are being applied in the design of the project.* |
| Justification | 1. Is the justification for the new data-handling unclear or unpublished?
 |   |  |  |  |
| *Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed 'for security reasons', or 'to prevent fraud', are much less likely to calm public disquiet*. |
| Identity | 1. Will the project require anyone to contact individuals in ways that they may find intrusive?
 |   |  |  |  |
| 1. Does the project involve an additional use of an existing identifier?
 |  |  |  |  |
| 1. Does the project involve use of a new identifier for multiple purposes?
 |   |  |  |  |
| 1. Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?
 |   |  |  |  |
| 1. Will the project result in anyone making decisions or taking action against individuals in ways which could have a significant impact on them?
 |  |  |  |  |
| *The public understands that an identifier enables an organisation to collate data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.* |
| Data | 1. Will the project involve the collection of new information about individuals?
 |  |  |  |  |
| 1. Will the project compel individuals to provide information about themselves?
 |  |  |  |  |
| 1. Will the project result in the handling of a significant amount of new data about each person, or are there plans to use the information for a purpose it is not currently used for, or in a way it is not currently used?
 |   |  |  |  |
| 1. Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?
 |   |  |  |  |
| 1. Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?
 |   |  |  |  |
| 1. What considerations have been made regarding the adequacy, relevance and necessity for the collection of each field of personal confidential data for the new system/process?
2. Please describe what has been done and the outcome.
 |  |  |  |  |
| *The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g. to support so-called 'front-end verification'), and the matching of personal data from multiple sources.* |
| Data Handling | 1. Does the project involve complex data controller in common arrangements that may prove difficult to administer?
 |  |  |  |  |
| 1. Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?
 |   |  |  |  |
| 1. Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?
 |   |  |  |  |
| 1. Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?
 |   |  |  |  |
| 1. Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?
 |   |  |  |  |
| 1. Does the project involve new or changed data retention arrangements that may be unclear or extensive?
 |   |  |  |  |
| 1. Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?
 |   |  |  |  |
| 1. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
 |  |  |  |  |
| 1. Are other organisations involved in the processing of the data?
 | If yes, please list below. |
| **Organisation name and Data Protection Register number.** | **Are they a Data Controller (DC) or Data Processor (DP)?** | **Compliance with the Data Security & Protection Toolkit (previously Information Governance Toolkit)** |
| **Completed****Y/N** | **Score****(%)** | **As at:****(Date)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Exemptions | 1. Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?
 |   |  |

# Section Four

This section relates to work that may be included within the overall project plan however if some planning has already taken place it should be recorded here.

|  |
| --- |
| **Questions for the procurement / development of a data collection system.** |
| 1. Has a data flow mapping exercise been undertaken?

If yes, please provide a copyIf no, please ensure one is included within the overall project plan | ***YES / NO (provide further actions to be taken)*** |
| 1. Does the system involve new or changed USER access controls and/or authentication requirements?
 | ***YES / NO (please provide details)*** |
| 1. Does the system allow different levels of access for different job roles?
 | ***YES / NO (please provide details)*** |
| 1. Are there any new or additional reporting requirements for this project?

If yes, please provide **full** detailsIf not yet considered please confirm it will be included in the overall project plan. | *Details to include, but not limited to: who is recipient? How reported? (Identifiable information, Pseudonymised[[1]](#footnote-1) or anonymised), whether aggregated or record level.*  |
| 1. Does the system affect any current policies in relation to the collection and management of PCD – in so far as it may require changes to policy?
 | ***YES/NO (please provide details)*** |
| 1. Who provides the data that will populate the system?
 | ***e.g. Patients, Staff, Other (please specify)*** |
| 1. How will you ensure that the individuals whose information will be processed have been informed of all the processing[[2]](#footnote-2) and disclosures that will take place?
 | ***Please provide details*** |
| 1. Will individuals be asked for consent for their information to be accessed, collected and/or shared?
 | ***YES/NO (please provide details)*** |
| 1. If NO to Q8, provide list the reason(s) for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has Section 251 approval or other legal basis,
 | ***Please provide full details and evidence*** |
| 1. If data is to be shared outside of the organisation will individuals be able to opt-out? How will the opt-out be recorded e.g. on the system, manual
 | ***YES/NO (please provide details)*** |
| 1. If this project relates to the disclosure of information, how will obligations to share be met?
 | ***Please provide details*** |
| 1. Who will have access to the identifiable information from the system/process and how?
 |  |
| 1. Have you considered an audit trail and what information it will capture? Examples include: all changes made to a record, who made the changes, who has viewed the record.
 | ***If YES please provide details, If NO, please provide details of plans to include this.*** |
| 1. What procedures are in place or planned for the rectifying of inaccurate data, blocking the use of data by individual request or court order?
 | ***Please provide details*** |
| 1. Is the new system replacing a system which is currently in use?

If YES, what is the name of the old (legacy) system? | ***YES/NO (please provide details)*** |
| 1. If yes to Q15, is all the data being migrated to the new system?

If yes, what has been done/will be done to ensure that the data is of good quality, appropriate, adequate and not excessive. | ***Please provide details:*** |
| 1. If no to Q15, what arrangements have been/will be made to ensure that controlled access is still available to records which have not reached their retention period.
 | ***Please provide details*** |
| 1. What arrangements are in place to manage the legacy system – is it being decommissioned, what is happening to the data it contains, do some staff need to continue to have access to it, how long will it be maintained etc.
 | ***Please provide details*** |
| 1. What considerations have been made/planned regarding the destruction of any records as part of this project?
 | ***Please provide details*** |
| 1. What is the proposed model for the storage of, and access to, records?

NB some of the options listed may go against our policy(s) and so will be highlighted in the report produced from this questionnaire |  Paper  Networked database, stored on organisations own server and access via network. Separate system with data saved on network Separate system with no network (standalone) Hosted on a third party server and accessed via internet/portal Other – please specify: |
| 1. If any information will be stored off-site (off-site means outside the organisation and its computer network) please provide details of information security arrangements
 | ***Please provide details of information security arrangements*** |
| 1. Will information be sent off-site (off-site means outside the organisation and its computer network)?
 | ***Please provide details*** |
| 1. Please state by which method the information will be transported
 |  Email (not nhs.net mail)  Fax nhs.net email  Courier Website access  Post (internal) Post (external)  By hand Telephone  Wireless network Secure internet connection (please specify) Other – please specify:  |
| 1. Is any personal information of any kind being transferred to a foreign country?
 | ***YES/NO – if YES please state where to and for what reason*** |
| 1. If yes to Q24, Specify the data that is to be transferred abroad
 |  |
| 1. Is the system to be covered by existing Information Security and other policies?
 | ***YES/NO******If NO, please state why and what other arrangements are being made/planned*** |
| 1. Is disaster recovery and contingency planning being put in place to manage the effect of any unforeseen events?
 | ***YES/NO*** |
| 1. Are there procedures in place to recover data which may be damaged through

- Human error- Computer virus- Network failure- Theft- Fire- Flood- Other disaster | ***YES/NO*** |
| 1. Has the requirement to apply clinical risk management to the deployment of patient based systems been addressed and in what ways?
 | ***Please provide details*** |
| 1. What assurances will be received to ensure Mandatory Staff Training is in place for the following:
* Data collection:
* Use of the System or Service:
* Collecting Consent:
* Information Governance?
 | ***Please provide details*** |

NB – Record retention is important and fundamental to DPA, though not included in DPIA questions; provision for retention and destruction should be made in line with normal care record retention requirements

Once completed, please return to;

***Insert details of who to return form to***

If you have any queries, please contact the IG team using the contact details detailed in Section 5 of this document.

# Section Five - Risk– To be completed by the IG Team Only

**DPIA Assessment ID:**

Please list the risks identified from Section, the scores and any actions that must be undertaken.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk Identified | Consequence Score1 = Low1 = Medium3 = High | Likelihood Score1 = Low2 = Medium3 = High | Risk Score (C x L) | Action | Owner | Target Date |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Section Six – DPA 2018 / GDPR – To be completed by the IG Team Only

Does the DPIA meet the following legal requirements?

|  |  |
| --- | --- |
|  | **Assessment of Compliance** |
| **Principle 1 –** Lawfulness, fairness and transparency |  |
| **Principle 2 –** Purpose limitation |  |
| **Principle 3 –** Data minimisation  |  |
| **Principle 4 –** Accuracy |  |
| **Principle 5 –** Storage limitation |  |
| **Principle 6 –** Integrity and confidentiality (security) |  |
| **Principle 7 –** Accountability  |  |

# Section Seven – Caldicott – To be completed by the IG Team Only

|  |  |
| --- | --- |
|  | **Assessment of Compliance** |
| **Principle 1 –** Justify the purpose(s) of using confidential information |  |
| **Principle 2 –** Only use it when absolutely necessary |  |
| **Principle 3 –** Use the minimum that is required |  |
| **Principle 4 –** Access should be on a strict need-to-know basis |  |
| **Principle 5 -** Everyone must understand his or her responsibilities |  |
| **Principle 6 –** Understand and comply with the law |  |
|  **Principle 7 -** The duty to share information can be as important as the duty to protect patient confidentiality |  |

# Statement of Assessment

|  |  |  |
| --- | --- | --- |
| Statement: Please select the appropriate statement and delete the words **in bold** that do not apply. The other statements should then be deleted. | Assessed By | Date |
| The privacy risks for this project/change have been assessed, based upon the information provided, and it is felt that there is a low risk of any impact to the privacy of the data subjects. Recommendations **have/have not** been made within this section which should be actioned to further reduce or restrict the privacy risks.  |  |  |
| The privacy risks for this project/change have been assessed, based upon the information provided, and further **Data Protection/Legal Compliance and/or small scale Privacy Impact checks** were undertaken. Recommendations **have/have not** been made within this section which should be actioned to further reduce or restrict the privacy risks. |  |  |
| The privacy risks for this project/change have been assessed, based upon the information provided, and a **full scale Data Protection Impact Assessment** should be undertaken. Actions have been included above which must be actioned before the project/change can be approved by the SIRO. |  |  |

**SIRO/Caldicott Guardian Statement of Assessment** – **for Full scale Data Protection Impact Assessments only**

|  |  |  |
| --- | --- | --- |
| Statement – Please remove **text in bold** that is not applicable | Please Tick | Date |
| Having reviewed the privacy impact risks, assessment recommendations and/or DPIA Report, I confirm that this project/change **can/cannot** proceed:The reasons for this are:* **It is crucial to the service delivery within the Trust/The privacy risks identified would impact negatively on the service delivery within the Trust**
* The mitigating recommendations, once completed, **will/will not** reduce the likelihood of the privacy risks occurring
* Reassurance has been sought from the Information Commissioners Office and the Information Governance Alliance, who have confirmed that we **are able to proceed/should not proceed** with this project/change.
 | [ ] [ ] [ ]  |  |

Once completed, please send the completed form back to the originator and keep a copy for record purposes.

# Appendix 3 - 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.
1. Pseudonymised: where identifiable data has been replaced with alternative unique data so that individuals cannot be identified without a pre-defined code/key which is retained in a separate secure place with strict access controls [↑](#footnote-ref-1)
2. Processing (as defined in the Data Protection Act 2018) in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as (a) collection, recording, organisation, structuring or storage, (b) adaption or alteration, (c) retrieval, consultation or use, (d) disclosure by transmission, dissemination or otherwise making available, (e) alignment or combination, or (f) restriction, erasure or destruction. [↑](#footnote-ref-2)