# 

# Data Protection Impact Assessment (DPIA)

Please follow this assessment at the planning stage of any new process or project that includes the processing of personal data.

**Examples of when a full DPIA is required include:**

* Introduction of a new information system for storing and accessing personal data
* Data sharing initiative between two or more organisations
* Initiatives to identify individuals within a specific demographic group for a particular course of action
* Re-use of personal data held by the Trust for a new purpose
* Providing access to personal data held by the Trust to any external third parties.

An effective DPIA will allow for the identification and remediation of data privacy issues at the early stages of a project, ensuring that principles of ‘privacy by design’ and ‘privacy by default’ are embedded across the Trust.

Please complete all questions with as much detail as possible (liaising with partners/third parties where necessary).

Advice regarding terminology and requirements can be provided by the Trust’s Information Governance (IG) team and their contact details are included on the IG intranet pages.

Once completed, the full DPIA form must be submitted to Rachael.smith@swyt.nhs.uk for approval.

**Section 1: DPIA general details**

|  |  |  |
| --- | --- | --- |
| **System/project/process (referred to as ‘project’) title:** | Staff vaccination and exemption status | |
| **Objective:**  Why is the project required?  Please indicate urgency and any key deadlines for project approval. | New legislation mandating COVID vaccination as a condition of employment from 1 April 2022 is driving this activity. The Trust will be legally required to ensure patient facing staff are vaccinated so need to obtain evidence to ascertain their vaccination and exemption status. This is a new data collection. | |
| **Stakeholders/Partners:**  Please outline the nature of such relationships and the corresponding roles of other organisations or third parties. | NHS England and NHS Improvement | |
| **Project lead:** | Name: | Julie Williams |
| Title: | Assistant Director |
| Department: | Corporate Governance |
| Telephone: | 07488323573 |
| Email | Julie.williams2@swyt.nhs.uk |
| **Information Asset Owner:**  All information systems/assets must have an [Information Asset Owner (IAO).](#IAO) IAO’s should normally be a Head of Department/Service. | Name: | Lindsay Jensen (for ESR) |
| Title: | Interim Director of HR & OD |
| Department: | Executive team |
| Telephone: |  |
| Email | Lindsey.jensen@swyt.nhs.uk |

**Section 2: DPIA key questions**

|  | **Question** | **Response** |
| --- | --- | --- |
| **Tell us about the data** | | |
|  | **Will the project involve the collection or processing of person identifiable data?**  If answered ‘No’ then a PIA is not normally suggested. | Yes  No  If yes, who will this data relate to?  Patient(s)  Staff  Other: Click here to enter text. |
|  | **Please state purpose for the processing of the data:**  For example, patient care, commissioning, research, audit. | To meet new legislation mandating COVID vaccination as a condition of employment from 1 April 2022; patient facing staff will be advised by secure email/letter to home address that their vaccination and exemption status will be downloaded directly from NIVS; details of evidence downloaded from NIVS will be uploaded to Sharepoint. In time, all data from Sharepoint will be extracted and migrated in bulk to ESR. Sharepoint at this point will be de-comissioned. |
|  | **Please tick the data items that are held in the system**  **Personal**    **Special categories**  **of personal data**  **(sensitive data)** | Name  Address  Post Code  Date of Birth  GP Practice  Date of Death  NHS Number  NI Number  Passport Number  Pseudonymised Data  Online Identifiers (e.g. IP Number, mobile device ID)    Health Data  Trade Union membership  Political opinions  Religion  Racial or ethnic origin  Sex life and sexual orientation  Biometric Data  Genetic Data    Other: Click here to enter text. |
|  | **Have any consultation/checks have been made regarding the adequacy, relevance and necessity for the processing of personal and/or sensitive data for this project? Please include details where relevant.** | The data collection is being driven by new legislation. Discussions have been held at national and regional level IG forums, with guidance from NHSX and the regional SIGN. The Trust’s approach is in line with these discussions. |
|  | **How will the data be kept up to date and checked for accuracy and completeness?** | Data will be downloaded directly from NIVS or sourced from NIVS. Any errors between NIVS and the Trust systems will be amended by the P&I Technical Team. |
| **Data processing** | | |
|  | **Will a third party organisation or supplier be involved in processing person identifiable data?** | Yes  No  If no, please go to the Confidentiality section at Q11. |
|  | **Is the third party registered with a supervisory authority, such as the Information Commissioners Office?** | Yes  No  Supervisory Authority: ICO  Registration Number: ZB287995 |
|  | **Is the third party registered and compliant with the Department of Health’s Data Security & Protection Toolkit (formally known as the** [**Information Governance Toolkit submission**](https://www.igt.hscic.gov.uk)**)?** | Yes  No  If yes, please give organisation code and percentage score:  Click here to enter text.  *IG Toolkit Score:*  Standards met  Unsatisfactory  If unsatisfactory, please request a copy of the improvement plan and enclose it with this assessment. |
|  | **Has the third party appointed a Data Protection Officer?** | Yes  No  If yes, please provide contact details:  england.dpo@nhs.net |
|  | **Does the third party/supplier contract(s) include all the necessary clauses regarding Data Security, Data Protection and Freedom of Information?**  See Procurement checklist. | Yes  No  Is the contract based on or utilise the NHS standard contract?  Yes  No  If no, please explain who has been involved in negotiation and agreement of contract terms:  Click here to enter text. |
|  | **Will other third parties (not already identified) have access to the data?**  Include any external organisations. | Yes  No  If so, for what purpose?    Please list organisations and by what means of transfer |
| **Confidentiality** | | |
|  | **Please outline how individuals will be informed and kept informed about how their data will be processed.**  Reference to [privacy/fair processing notice and/or leaflets](https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/) must be included. | Full explanation and privacy statement will be provided to all impacted individuals. |
| 1. **le** | **Does the project involve the collection of data that may be considered intrusive?**  Are all data items clearly defined? Is there a wide range of ‘sensitive data’ (see Q3 above) being included? | Yes  No  If yes, please explain:  The Trusts will be processing and maintaining staff vaccination and exemption status to ensure business readiness by the 1/4/2022 mandatory Vaccination deadline. |
|  | **Are you relying on individuals (patients/staff) to consent to the processing of personal identifiable or sensitive data?**  Where applicable, please provide copies of any consent documentation that will be used, including patient information leaflets. | Yes  No  **Where consent *is* being sought:**  Is the consent [explicit](#ExplicitCons)?  Yes  No  How will consent be obtained and by whom?  Initially consent was sought however this DPIA is now in place to ensure the Trust can plan effectively for the mandatory vaccine deadline for all colleagues, including those who have not consented. A copy of the original letter is attached for completeness. This is in line with (can we state again how we feel justified to do this)  How will consent, non-consent, objections or opt-outs be recorded and respected?  Please see previous letter sent  Where explicit consent is *not* being sought:  a. Will identifiable data only be handled within the patients’ direct care team (in accordance with the [Common Law Duty of Confidentiality](#CommonLaw))?  Yes  No  b. Which legal basis/justification is in place to permit this processing (in accordance with [Data Protection Act](#DPA)/[General Data Protection Regulation](#GDPR))?  Direct Patient Care  Public Interest  Safeguarding  NHS Act 2006 (Section 251)  Court Order  Other: Click here to enter text. |
|  | **What arrangements are in place to process Subject Access Requests?**  What would happen if such a request were made, i.e. where individuals requests copies of their information? | The request would go through HR |
|  | **Will the processing of data be automated?**  Will the project involve automated processing or profiling of personal data to determine an outcome for the individual? | Yes  No  Not applicable  If yes, please outline what arrangements are available to enable the individual access and to extract data (in a standard file format).  Specific access by the performance & information teams to provide reporting.  Please also detail any profiling that may take place as part through automated processing:  none |
|  | **What process is in place for rectifying/blocking data?**  What would happen if such a request were made? | If data is incorrect, the Trust’s DPO will be contacted in the first instance |
|  | **Does the project involve any new information sharing between stakeholder organisations?** | Yes  No  If yes, please describe:  Vaccination and exemption status will be downloaded directly from NIVS;; details of evidence downloaded from NIVS will be uploaded to Sharepoint. In time, all data from Sharepoint will be extracted and migrated in bulk to ESR. Sharepoint at this point will be de-comissioned. ESR is checked against the payroll system to confirm accuracy.  **If you have one, please provide a data flow diagram showing how identifiable information would flow.** |
|  | **Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?**  The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a collection of a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously). | Yes  No  **If yes,** **please ensure this is demonstrated in the response at Q17 above.** |
| **Information Security** | | |
|  | **Who will have access to the data being processed?**  Please refer to roles/job titles/departments. Include internal users, third parties, partner organisations etc. | Assistant Director of Corporate Governance. HR Systems team, P&I team, HR Services team, Head of HR Operations, HR Business Partners, Interim Director of HR & OD, Vaccination Program Lead; ESR – data is held within a particular module that line managers do not have access to; Sharepoint – only authorised staff have access to this system. The list of authorised users is reviewed regularly. |
|  | **Is there a useable audit trail in place for the use of data?**  For example, to identify who has accessed a record? | Yes  No  Not applicable  If yes, please outline the audit plan:  The audit trail is via Sharepoint cross checked with ESR. |
|  | **Provide details of both the physical and technical security measures being taken to protect the data, i.e. wherever it is stored or accessed?** | Unique login credentials |
|  | **Please indicate all methods in which data will be transferred** | Fax  Email (Unsecure/Personal)  Email (Secure/nhs.net)  Internet (unsecure – e.g. http)  Telephone  Internet (secure – e.g. https)  By hand  Courier  Post – track/traceable  Post – normal  Other: |
|  | **Is the technology supported by the supplier or internal IT Department?** | Yes  No  Not applicable  If yes, please outline how these IT support requirements will be confirmed prior to any ‘go-live’ operational use:  Internal IT have responsibility for ESR & Sharepoint Systems in this process |
| **Privacy and Electronic Communications Regulations** | | |
|  | **Will the project involve the sending of unsolicited marketing messages electronically such as telephone, fax, email and text?**  [Please note that seeking to influence an individual is considered to be marketing.](#PECR) | Yes  No  If yes, what communications will be sent?  Click here to enter text.  Will consent be sought prior to this?  Yes  No  If no, please explain why consent is not being sought first:  Click here to enter text. |
| **Records Management** | | |
|  | **What steps will be taken to ensure that relevant data records are accurate, complete and up to date?** | Data will be downloaded directly from NIVS to cross check with our internal systems. Any errors will be amended by the P&I technical team only. |
|  | **What are the specific retention periods for this data?**  Please refer to the [Records Management Code of Practice for Health and Social Care 2016](https://digital.nhs.uk/media/1158/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016/pdf/Records-management-COP-HSC-2016) and list the retention period for datasets relevant to this project. | Data will remain on sharepoint until the system is decommisioned (likely 12 month period). Once transferred from Sharepoint, data will remain on the ESR record as per the Records Management Code of Practice retention schedule for employee records. |
|  | **Will the data be securely destroyed when it is no longer required?** | Yes  No  If no, please detail: Click here to enter text. |
| **Business Continuity** | | |
|  | **Have business continuity requirements been considered?**  Considerations must be given to a range of business continuity scenarios including: systems being unavailable, data loss or damage (e.g. IT failure). | Yes  No  Business Continuity is not applicable  Please explain and either reference how such plans link with the organisational plan or why there are no business continuity considerations that are applicable for this project: Sharepoint Business Continuity Plan will apply; ESR Business Continuity Plan will apply |
| **Data Processing Outside of the EEA** | | |
|  | **Will any personal and/or sensitive data be transferred to a country outside the European Economic Area (**[**EEA**](#EEA)**)?** | Yes  No  If yes, which data and to which country?  Click here to enter text.  If yes, are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?  Yes  No  If yes, who completed and determined this?  Click here to enter text. |

**Section 3: Review and Approval**

**Assessment completed by:**

|  |  |
| --- | --- |
| **Name:** | Julie williams |
| **Title:** | Assistant Director |
| **Sent electronically or Signed:** |  |
| **Date:** |  |

030122

**Assessment reviewed by Information Asset Owner (IAO) (see appendix glossary for further details).**

|  |  |
| --- | --- |
| **Name:** |  |
| **Title:** |  |
| **Reviewed electronically or Signed:** | The IAO review and endorsement is attached. |
| **Date:** |  |

**Assessment approved by:**

|  |  |
| --- | --- |
| **Name:** | Rachael Smith |
| **Title:** | Data Protection Officer |
| **Electronic Approval or Signature** | Data Protection Officer approval is attached. |
| **Date:** | Click here to enter text. |

|  |  |
| --- | --- |
| **Name:** | Darryl Thompson |
| **Title:** | Director of Nursing, Quality & Professions / Caldicott Guardian |
| **Electronic Approval or Signature** | Caldicott Guardian approval is attached. |
| **Date:** | Click here to enter text. |

# Appendix A: Example risks

**Risks to individuals**

1. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
2. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
3. New surveillance methods may be an unjustified intrusion on their privacy.
4. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
5. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
6. Identifiers might be collected and linked which prevent people from using a service anonymously.
7. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
8. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
9. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
10. If a retention period is not established information might be used for longer than necessary.

**Corporate risks**

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

**Compliance risks**

1. Non-compliance with the Data Protection Act 1998/General Data Protection Regulation (EU) 2016/679.
2. Non-compliance with the Common Law Duty of Confidentiality.
3. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
4. Non-compliance with Human Rights Act 1998 and Equality Act 2010.

# Appendix B: Glossary

|  |  |
| --- | --- |
| ***Item*** | ***Definition*** |
| **Anonymity** | Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients. |
| **Authentication Requirements** | An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks. |
| **Caldicott** | Seven Caldicott Principles were established following the original reviewed in 1997 and further development in 2013. The principles include:   1. justify the purpose(s) 2. don't use patient identifiable information unless it is necessary 3. use the minimum necessary patient-identifiable information 4. access to patient identifiable information should be on a strict need-to-know basis 5. everyone with access to patient identifiable information should be aware of their responsibilities 6. understand and comply with the law 7. the duty to share information can be as important as the duty to protect patient confidentiality |
| **Common Law Duty of Confidentiality** | This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:   * Where the individual to whom the information relates has consented * Where disclosure is in the overriding public interest; and * Where there is a legal duty to do so, for example a court order * The common law applies to information of both living and deceased patients. |

|  |  |
| --- | --- |
| **Data Protection Act 1998 (fully applicable up to 25 May 2018)** | The DPA defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must:   1. be processed fairly and lawfully. 2. be obtained only for lawful purposes and not processed in any manner incompatible with those purposes. 3. be adequate, relevant and not excessive. 4. be accurate and current. 5. not be retained for longer than necessary. 6. be processed in accordance with the rights and freedoms of data subjects. 7. be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. 8. not be transferred to a country or territory outside the European Economic Area unless that country or territory protects the rights and freedoms of the data subjects. |
| **European Economic Area (****EEA)** | The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway |
| **Explicit consent** | Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information. |
| **General Data Protection Regulation (EU) 2016/679 Principles of Lawful Processing of Personal Identifiable Information** | The GDPR requires that data controllers ensure personal data shall be:   1. processed lawfully, fairly and in a transparent manner in relation to individuals 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 not be considered to be incompatible with the initial purposes 3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed 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 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 insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals 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 |
| **IAO (Information Asset Owner)** | These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they ‘own’ and to provide assurance on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area. |
| **Implied consent** | Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure. Implied consent is unique to the health sector and may be revised under the GDPR. |
| **Information Assets** | Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware. |
| **Information Risk** | An identified risk to any information asset that the organisation holds. Please see the Risk Policy for further information. |
| **Personal Data** | This means data which relates to a living individual which can be identified:   1. from those data, or 2. from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller.   It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual |
| **Privacy and Electronic Communications Regulations 2003** | These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information. |
| **Privacy Invasive Technologies** | Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk |
| **Pseudonymisation** | Where patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. |
| **Records Management: NHS Code of Practice** | Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule. |
| **Retention Periods** | Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives. |
| **Special categories of personal data (sensitive data)** | This means personal data consisting of information as to the:   1. Concerning health, sex life or sexual orientation 2. Racial or ethnic origins 3. Trade union membership 4. Political opinions 5. Religious or philosophical beliefs 6. Genetic data 7. Biometric data |
|  |  |