# 

# Data Protection Impact Assessment (DPIA)

Please complete all questions with as much detail as possible (liaising with partners/third parties) and then contact the IG Team prior to seeking approval.

**Section 1: System/Project General Details**

|  |  |  |
| --- | --- | --- |
| **System/project/process (referred to thereafter as ‘project’) title:** | Familial hypercholesterolemia (FH) patient identification | |
| **Objective:** | To identify those at risk of FH, and possibly their relatives, to ensure patients are treated as appropriate and supported to manage their condition | |
| **Detail:** Why is the new system/change in system required? Is there an approved business case? | The project will proactively find patients from GP Systems identified as being at risk of FH to ensure they are treated and supported appropriately. The treatment and ongoing interactions to be provided initially at the GP Practice. | |
| **Stakeholders/Relationships/Partners:** Please outline the nature of such relationships and the corresponding roles of other organisations. | Patients and their relatives; GP Practice - have the patient records that will be checked; FH service - provide and facilitate the project; NEL CCG and York Hospital NHS Foundation Trust - support, facilitate and have governance responsibility for the project. | |
| **Other related projects:** | none | |
| **Project Lead:** | Title: | Commissioning Officer |
| Department: | Service planning and redesign |
| **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. |  | |
| Title: | Caldicott Guardian |
| Department: | Chantry Practice |
| Telephone: | 01472 264980 |
|  |  |
| **Information Asset Administrator:**  Information systems/assets may have an [Information Asset Administrator (IAA)](#IAA) who reports the IAO. IAA’s are normally System Managers/Project Leads. | Title: | Information Asset Manager |
| Department: | Chantry Practice |
| Telephone: | 01472 264980 |

**Section 2: Data Protection Impact Assessment Key Questions**

|  | **Question** | **Response** |
| --- | --- | --- |
| **Data Items** | | |
|  | **Will the project use identifiable or potentially identifiable data in any way?**  If answered ‘No’ then a DPIA is not normally suggested. | Yes  No  If yes, who will this data relate to:  Patient  Staff  Other: Click here to enter text. Possibly relatives, if named |
|  | **Please state purpose for the processing of the data:**  For example, patient care, commissioning, research, audit, evaluation. | For improved/targeted patient care for identified individuals and the potential identification of family members who might benefit from assessment |
|  | **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: |
|  | **What consultation/checks have been made regarding the adequacy, relevance and necessity for the processing of the data for this project?** | The patient record is required so that health care professionals can make a fully informed decision based on clinical background and history before the patient (and potentially their relatives) are identified as being at risk of FH. |
|  | **How will the data be kept up to date and checked for accuracy and completeness?** | The patient record stored on the GP clinical system will be updated once the identification and decision regarding intervention/treatment has been made |
| **Data processing** | | |
|  | **Will a third party be processing data on the CCG or one of its contractors?** | Yes  No  If no, please go to the Confidentiality section. |
|  | **Is the third party contract/supplier of the project registered with the Information Commissioner?**  This was required until 25 May 2018. | Yes  No  Organisation: York Teaching Hospital NHS Foundation Trust  Data Protection Registration Number: Z4819561 |
|  | **Has the third party supplier completed and published a satisfactory** [**Data Security and Protection Toolkit submission**](https://www.dsptoolkit.nhs.uk/)**?**  Please note that the Data Security and Protection Toolkit replaced the IG Toolkit from 1 April 2018. | Yes  No  If yes, please give organisation code and percentage score:  All GP practices have published a toolkit for 2018/19 and standards met  York Teaching Hospital NHS Foundation – standards met  Organisation code RCB  *IG Toolkit Score:*  Satisfactory  Not satisfactory  Satisfactory with Improvement Plan  If satisfactory with an improvement plan, please request a copy of the plan and enclose it with this assessment.  If not satisfactory, please explain how the service has been procured:  Click here to enter text. |
|  | **Does the third party/supplier contract(s) include all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** See [Contract and Commissioning Information Governance Assurance](#SupportingDocs) checklist. | Yes  No  Is the contract based on or utilise the NHS standard contract?  Yes  No |
|  | **Will other third parties (not already identified) have access to the data?** Include any external organisations. | Yes  No  If so, for what purpose?  For patient care  Please list organisations and by what means of transfer:  Yorkshire and Humber Familial Hypercholesterolaemia Service: York Teaching Hospital NHS Foundation Trust, Data Protection Registration Number: Z4819561 – electronic transfer. All will be NHS mail to NHS mail, therefore secure. In the unlikely event of a non-NHS mail transfer, NHS encryption will be used. |
| **Confidentiality** | | |
|  | **Please outline how individuals will be informed and kept informed about how their data will be processed.**  A copy of the [privacy notice and/or leaflets](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) must be provided. | The patient record stored on the GP clinical system will be updated once the identification and decision regarding intervention/treatment has been made. Patients will be made aware that their data is being accessed in connection with this project. The way in which this is done will be subject to discussion with practices. An addition to Privacy Notice could give details of overall project with more explicit information provided to those selected for full assessment |
|  | **Does the project involve the collection of data that may be unclear or intrusive?** Are all data items clearly defined? Is the data collected limited to a specific set of predefined categories? | Yes  No  If yes, please explain:  Click here to enter text. |
|  | **Are you relying on individuals (patients/staff) to explicit consent to the processing of personal identifiable or sensitive data?**  Please provide copies of any consent documentation that will be used, including patient information leaflets | Yes  No (Go to next question)  How will consent be obtained and by whom?  Usual GP practice procedures for obtaining consent will be used from individuals identified as potentially benefiting from an assessment  Will the consent cover all proposed processing and sharing/disclosures?  Yes  No  If no, please detail:  1. Using an algorithm to extract initial information to identify potential subjects - I think this would be covered under public tasks - consent would not be necessary but the Privacy Notice should reference the project with a link to more information.2. Liaising between clinicians about patients identified as being at risk of FH and any ongoing treatment plans etc - Patient care - no formal consent necessary3. Identification of relatives and referrals for DNA testing - would require informed consent at practice level. |
|  | **If explicit consent is not being sought, what legal basis enables this data processing?**  For more information about conditions for processing, please see the [ICO’s GDPR website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/). | Personal data (identifiers and potentially identifiable data):  Relating to a contract: Click here to enter text.  Legal obligation: Click here to enter text.  Vital interests: Click here to enter text.  Public task: Click here to enter text.  Other: Click here to enter text.  Special categories of personal data (sensitive data), *if applicable*:  Medical related: Click here to enter text.  Public Health: Click here to enter text.  Employment related: Click here to enter text.  Vital interests: Click here to enter text.  Already public: Click here to enter text.  Legal claim related: Click here to enter text.  Substantial public interest: Click here to enter text.  Other: Click here to enter text. |
|  | **Will identifiable data only be handled within the patients’ direct care team (in accordance with the** [**Common Law Duty of Confidentiality**](#CommonLaw)**)?** | Yes  No  If no, please detail:  Trained qualified nursing staff at York Teaching Hospitals NHS Foundation Trust will have access to the records of patient’s selected for assessment |
|  | **How will consent, non-consent, objections or opt-outs be recorded and respected?** | On the GP clinical system |
|  | **What arrangements are in place to process Subject Access Requests?** What would happen if such a request were made? | GP Practices and York Teaching Hospitals NHS Foundation Trust will have a Subject Access Request policy in place |
|  | **Will the processing of data be automated?** Will the proposed processing of data involved automated means of processing 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). Please also detail any profiling that may take place as part through automated processing:  Click here to enter text. |
|  | **What process is in place for rectifying/blocking data?** What would happen if such a request were made? | Subject Access Request and Data Protection policies will be adhered to. If a patient does not wish to be involved, their details will not be included in the project from the outset. If a patient decides at any point they no longer wish to be involved, their details will be removed from the study data. |
| **Engagement** | | |
|  | **Has stakeholder engagement taken place?** | Yes  No  If yes, how have any issues identified by stakeholders been considered?  GP meeting 13 March 2019. Meeting held with consultant at Diana Princess of Wales hospital on 8 October 2019.  No issues identified.  If no, please outline any plans in the near future to seek stakeholder feedback:  Click here to enter text. |
| **Data Sharing** | | |
|  | **Does the project involve any new data sharing between stakeholder organisations?** | Yes  No  If yes, please describe: Data will be shared between the GP practice and Yorkshire and Humber Familial Hypercholesterolaemia Service. The data is flowing from the practice directly to the FH service electronically and securely by NHS mail. |
| **Data Linkage** | | |
|  | **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 provide a data flow diagram showing how identifiable information would flow and ensure this is added to the CCG Information Asset and Data Flow Register (see Information Assets and Data Flows section). |
| **Information Security** | | |
|  | **Who will have access to the data within the project?**  Please refer to roles/job titles/organisations. | GPs, practice nurses, administrative staff in GP practices, FH nurses |
|  | **Is there a useable audit trail in place for the project?**  For example, to identify who has accessed a record? | Yes  No  Not applicable  If yes, please outline the audit plan: Audit of access is stored on GP clinical systems |
|  | **Where will the data be kept/stored/accessed?**  Where applicable, please refer to data flow diagram. | The practice advises patients that: ‘Risk stratification data tools are increasingly being used in the NHS to help determine a person’s risk of suffering a particular condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from a number of sources including NHS Trusts and from this GP Practice. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way.’ When the information is transferred to the FH service, it will be stored on systems that are DSP toolkit compliant. Access will be restricted to authorised staff only on a basis of least privilege. |
|  | **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  Software  Mobile app  Other: Click here to enter text. |
|  | **Does the project involve privacy enhancing technologies?**  *New forms* of encryption, two factor authentication and/or pseudonymisation. | Yes  No  If yes, please give details: Click here to enter text. |
|  | **Is there a documented System Level Security Policy (SLSP) or process for this project?**  A [SLSP](#SupportingDocs) is required for new *systems* – this is likely to need to be completed by the supplier. | Yes  No  Not applicable  If yes, please provide a copy. |
| **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 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/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016) and list the retention period for identifiable project datasets. | In line with the Record Management code of practices for NHS - 10 years |
|  | **Will the data be securely destroyed when it is no longer required?** | Yes  No  If no, please detail: Click here to enter text. |
| **Information Assets and Data Flows** | | |
|  | **Has an** [**Information Asset Owner**](#IAO) **been identified and does the** [**Information Asset**](#InfoAssets) **and Data Flow Register require updating?**  Please see the [Information Asset Register and Data Flow Mapping Form](#SupportingDocs). | Yes  No  If yes, include the completed Information Asset Register.  This will be identified and recorded via the practice. In respect of this service the practice Caldicott Guardian would be the IAO.  Does this project constitute a change to existing Information Asset(s) or is this a new Information Asset?  Yes  No  If yes, include the completed Information Asset Register and Data Flow Mapping Form for risk review. |
| **Business Continuity** | | |
|  | **Have the business continuity requirements been considered?** | 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: Plan to contact clinicians/primary care and the secondary team at Diana Princess of Wales Hospital (DPOW) regarding the possible increase if referrals as a result of patients identified as a result of the project |
| **Open Data** | | |
|  | **Will identifiable/potentially identifiable from the project be released as Open Data (placed in to the public domain)?** | Yes  No  If yes, please describe: Click here to enter text. |
| **Data Processing Outside of the UK and European Union (EU)** | | |
|  | **Will any personal and/or sensitive data be transferred to a country outside the UK?** | Yes  No  If yes, which data and to which country?  Click here to enter text. |

**Section 3: Data Protection Impact Assessment Information Governance Review**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Information Governance Review (for completion by IG)** | | | | **Response (for completion by project lead)** | |
| **Issue** | | **Potential Risk** | **Recommendation** | **Agreed Action** | **Completion (Date and Initials)** |
| **1** | Consent | Processing and sharing information with patient awareness | Agree with practice how this will be achieved | The practice will send a letter to patients to advise they have been identified by the search and to request consent for the data to be shared with the FH service. | 4/10/2019 |
| **2** |  |  |  |  |  |
| **3** |  |  |  |  |  |

*For completion by IG:*

**IG review completed by:**  Senior Information Governance Specialist **Review date:**  05/09/2019

**Date complete and risk assessed** 05/09/2019

**Section 4: Review and Approval**

**Assessment reviewed by**

|  |  |
| --- | --- |
| **Title:** | Senior Information Governance Specialist |
| **Date:** | 5.9.2019 |

**Data Protection Officer Review:**

|  |  |
| --- | --- |
| **Name:** | Paul Ellis |
| **Title:** | Data Protection Officer for NEL CCG |
| **DPO advice:**  **DPO should advise on compliance, risks identified and whether processing can proceed.**  **If accepting any residual high risk, consult the ICO before going ahead** | There is a clear and legitimate purpose for the processing of personal data to identify those at risk of FH, and ensure appropriate treatment and supported is offered / provided. The basis for processing is task in the public interest / provision of health care, with consent in accordance with established GP practice obtained from individuals identified as potentially benefiting from an assessment. All partners to the processing / sharing are DS&P Toolkit complaint and appropriate controls are in place to ensure the confidentiality, protection and security of the personal data shared which is limited to that personal data including special categories which is necessary for the purpose. I would recommend that processing can proceed. |
| **Approved:** | Yes |
| **Date:** | 7/11/2019 |

**SIRO/Caldicott Guardian Approval:**

|  |  |
| --- | --- |
| **Name:** | Jan Haxby |
| **Title:** | SIRO |
| **DPO advice accepted or overruled:**  If overruled, you must explain your reasons | Just a few points identified above to gain further clarity on. Clarity confirmed and SIRO approval. |
| **Approval:** | Yes |
| **Date:** | 03/12/2019 |