# Privacy Impact Assessment - Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| Key Information – please be as comprehensive as possible. | | | |
| Project Name: | High Intensity Use | | |
| Description of project: | A High Intensity Use Lead will:   * Effectively identify and work with people who have High Intensity Use of healthcare services such as the ED, 999 or high admissions within the ICB footprint. * Establish, utilise and coordinate stakeholders from multiple agencies – community, health, social and mental health to support clients physical, social and mental wellbeing. * Demonstrate a reduced workload on unscheduled care services and the wider health economy resulting from reduced 999 calls, which otherwise would have attended A&E, result in an admission. * To safely manage and coordinate the chaotic and demanding nature of the client group through the use of multi-agency support and the volunteer sector. * To provide fertile commissioning intelligence across all providers. * Lower the stigma associated with High Intensity Use. * Coordinate a replicable service which can be integrated and managed over the longer term across other providers. | | |
| Will the project involve any data from which individuals could be identified (including pseudonymised data)?  **(Yes/No)** | | | Yes |
| **IF NO THEN YOU DO NOT NEED TO ANSWER ANY FURTHER QUESTIONS AND A PIA IS NOT REQUIRED.** | | | |
| Key Contacts | | | |
| Project Manager Name & Job Title: | |  | |
| Project Manager Email: | |  | |
| Project Manager Phone: | |  | |
| Key Stakeholder Names & Roles: | |  | |

|  |  |
| --- | --- |
| Screening Questions | YES or NO |
| Will the project involve the collection of **new** information about individuals? | No |
| Will the project compel individuals to provide information about themselves? | No |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | Yes |
| Are you using information about individuals for a new purpose or in a new way that is different from any existing use? | Yes |
| 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. | No |
| Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services | Yes |
| Is the information to be used about individuals’ health and/or social wellbeing? | Yes |
| Will the project require you to contact individuals in ways which they may find intrusive? | Yes |

If any of the screening questions have been answered “YES”, then please continue with the Privacy Impact Assessment Questionnaire (below).

If all questions are “NO”, please return the document to the Information Governance Team and **do not** complete a Privacy Impact Assessment. Please email the completed screening to **………**

# Appendix F - Privacy Impact Assessment – Questionnaire

|  |  |
| --- | --- |
| **Use of personal information** | |
| **Description of data:** | Name  DOB  Telephone number  GP Practice Name/Branch  GP Practice Code  NHS Number  Ambulance Service Incident Number  Number of A&E contacts and Non-elective admissions |
| **What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?** | To support he delivery of *Direct Client Health Care* provided by (host org) through access to (Hospital) paper and electronic client health records.  The group of clients identified as high volume callers are amongst the most vulnerable in our society and must be identified and supported to present further harm and promote wellbeing. |
| **Will the information be new information as opposed to using existing information in different ways?** | Existing information is used in different ways. |
| **What is the legal basis for the processing of identifiable data?**  **If consent, when and how will this be obtained and recorded?** | *e.g. explicit data subject consent, s251 support, statutory power.*  Schedule 3 (8) DPA 1998 processing is necessary for medical purposes. Whilst some medical needs of these clients are being met, there is an unmet need resulting in repeat unscheduled and emergency care contacts. The parties are intending to improve health and care outcomes.  An individual data sharing agreement will be obtained by all clients involved in the project. |
| **Who will be able to access identifiable data?** | *This should include details of any data processors / contractors and sub-contractors and any proposed overseas transfers*.  The nominated lead(s) on the High Intensity Use Project |
| **Will the data be linked with any other data collections?** | *Please specify and provide business reason / information requirement*  Linked to SUS data - A&E and inpatient SUS data sets. |
| **How will this linkage be achieved?** | *Who will undertake the linkage and using what identifiers?*  Using the NHS number |
| **Is there a legal basis for these linkages?** | *i.e. is it within the terms of any prior consent? Is it within the scope of any statutory justification?*  Schedule 3 (8) DPA 1998 processing is necessary for medical purposes. Whilst some medical needs of these clients are being met, there is an unmet need resulting in repeat 999 calls, A&E attendances or non-elective admissions. The parties are intending to improve health and care outcomes. |
| **What security measures will be used to transfer the data?** | * Electronic data transfer – Information accessible via (hospital) Department Information System, Alert and (hospital) Client Administration System (PAS) created through (hospital) interactions with the client. * Physical access added to identification badges. * Secured email for sending HIU reports * End-to end-nhs.net to email information to GP Practice PM/Lead GP. * Practice (PM) updates information to Data Central secure repository |
| **What confidentiality and security measures will be used to store the data?** | *i.e. contractual arrangements with data processors, contractual arrangements with their staff as well as physical and technical security measures*  Data initially stored in host secure systems.  Note made on the client record within secure systems. |
| **How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?** | *e.g. Data retention, redaction, and disposal policy. Include arrangements if the project is withdrawn/ stopped*.  Each organisation will, as Data Controller for the information they hold, be responsible for its appropriate retention and disposal, both agree that such decisions will comply with:  Records Management, NHS Code of Practice, Part 2  Second edition (January 2009)  Destroyed as above and in accordance with: Destruction and Disposal of Sensitive Data Good Practice Guidelines, currently version 3.0, Date March 2015 |
| **What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only** **disclosed with consent or another legal basis?** | *e.g. oversight body / committee, security audit and risk review procedures.*  *This should also include contingency planning against accidental loss, destruction, or damage to personal data.*  Each party will have IG policies and protocols regarding confidentiality and security of information assets and data flows. These are assured via the IG toolkits submissions and monitored by each party.  Disclosure of final output from (host or hospital) to ICB is in a non-identifiable form. |
| **If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA?**  **Is there functionality to respect objections/ withdrawals of consent?** | *This should include how personal data is located and procedures for explaining the information in the record e.g. coded data, to the individual.*  *How third party and seriously harmful information will be handled and how grounds for withholding information will be managed.*  Parties will use their own subject access processes to ensure individuals can exercise their rights under the 6th principle.  Where a client is contacted, explicit consent will be sought, if this is refused the Project lead will advise the practice of the same. |
| **Are there any plans to allow the information to be used elsewhere either in the ICB, wider NHS or by a third party?** | No. The ICB will only receive non identifiable information. |
| **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. | |
| **Does any data flow in identifiable form? If so, from where, and to where?** | 1. Ambulance service to HIU lead 2. Practices (add NHS Number) to HIU lead 3. A&E BI team to HIU Lead 4. HIU Lead to A&E BI team 5. (host) to ICB (non identifiable) |
| **Media used for data flow**  **(e.g. email, fax, post, courier, other – please specify all that will be used)** | 1. Secure nhs.net email 2. Uploaded via data central secure repository 3. Secure nhs.net email notification/via data central repository |
| **Consultation requirements**  Part of any project is consultation with stakeholders and other parties. In addition to those indicated “Key information, above”, please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information.  It is the project’s responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations. | |
| Ambulance service, GP practices, clients via contact with HIU lead at which point explicit consent will be sought and they have the option to refuse to engage in process | |

|  |
| --- |
| **Step 6: Identify Privacy Solutions**  Describe the actions you could take/are taking to reduce the risks, and any future steps which would be necessary.  List any identified risks to privacy and personal information of which the project is currently aware. Risks should also be included on the project risk register. |

| **Risk Description**  **(to individuals, to the organisation or to wider compliance)** | **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?** |
| --- | --- | --- | --- |
| ***The 1st principle of the DPA is breached***  *Personal data shall be* ***processed fairly*** *and* ***lawfully*** *and, in particular, shall not be processed unless – (a) at least one of the conditions in* ***Schedule 2*** *is met, and (b) in the case of sensitive personal data, at least one of the conditions in* ***Schedule 3*** *is also met.* | ***Fair and lawful -*** *explicit consent usually by a phone call from the client by HIU Lead and this will be noted on client record and case file.*  ***Schedule 2 condition*** *- 2(1)* ***consent*** *and 2(6)* ***legitimate interests***  *Schedule 3 condition – 3(1)* ***explicit consent*** *and 8(1)(b)* ***medical diagnosis*** *and 8(1)(d)* ***the provision of health and treatment*** | *Eliminated*  *Eliminated*  *Eliminated* | *Yes*  *Yes*  *Yes* |
| ***The 2nd principle of the DPA is breached***  *Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.* | *Sharing information collected for healthcare and using this information for the same purpose is not an incompatible purpose.*  *Furthermore, if there was any ambiguity about this the explicit consent from clients removes any doubt.* | *Eliminated* | *Yes* |
| ***The 3rd principle of the DPA is breached***  *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.* | *A working group of professionals have carefully scrutinised the information sharing requirements to ensure only relevant and the minimum information required to improve client care is shared.* | *Eliminated* | *Yes* |
| ***The 4th principle of the DPA is breached***  *Personal data shall be accurate and, where necessary, kept up to date.* | *The parties will agree upon the following elements of data quality:* ***Accuracy***  *The parties will take reasonable steps and have internal processes in place to ensure, as far as is reasonably practical, that the information shared is accurate.*  ***Validity***  *Before sharing information, the parties will define the formats, conventions and definitions etc... to be applied to the information shared and will use a common template for this purpose.*  ***Reliability*** *Any changes to the way the information is collected will be communicated to all parties in advance as this may have impact the quality of information.*  ***Timeliness*** *The information is to be provided at a frequency considered sufficient to enable the objectives of the contact.*  ***Relevance and Completeness*** *The parties have agreed the data set collected (via the agreed template) is both adequate and relevant to achieve the objectives. It will be reviewed at least annually to determine it continues to be relevant and fit for purpose.*  *If at any time any party determines the information shared is no longer achieving the stated purposes immediate action will be taken to address and remedy this.* | *Reduced* | *Yes. The parties recognise information should be sufficiently accurate for its purposes.*  *The need for accuracy must be balanced with the importance of the uses of the information and the detrimental effect that inaccurate information would have on individuals. E.g. sometimes it may be acceptable to have some degree of inaccuracy, however at other times it will be unacceptable.*  *The Parties will ensure they have processes in place to ensure the information they hold and share is as accurate as it needs to be.* |
| ***The 5th principle of the DPA is breached***  *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.* | *The information will held by in accordance with the retention periods established by the parties IG policies and procedures and the NHS Records Management Code of Practice Part 2* | *Eliminated* | *Yes* |
| ***The 6th principle of the DPA is breached***  *Personal data shall be processed in accordance with the rights of data subjects under this Act.* | *The parties will use the subject access procedures established by each of the parties* | *Eliminated* | *Yes* |
| ***The 7th principle of the DPA is breached***  *Appropriate technical and organisational measures shall be taken against*  *unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.* | ***Storage and transfer of information***  *It is envisaged that the main risk lies in the transferring and holding of information between the parties safely and securely. All the data transfers are secure means either via nhs.net or held securely by (hospital / host) which provides a secure environment via Information Security standards (ISO27000). Data is shared between named individuals at (host) and GP practices.* | *Eliminated* | *Yes* |
| ***The 8th principle of the DPA is breached***  *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.* | *It is not envisaged that information will ever be transferred outside of the UK.* | *Eliminated* | *Yes* |

|  |  |  |
| --- | --- | --- |
| Step 7: Sign off and record the PIA outcomesWho has approved the privacy risks involved in the project? What solutions need to be implemented. | | |
|  | | |
| Risk | Approved solution | Approved by |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Privacy Impact Assessment completed by: | | |
| |  |  | | --- | --- | | Name: |  | | Position: |  | | Organisation: |  | | Address/ Location: |  | | Email: |  | | Phone: |  | | Date: |  | | | |