# **Risk mitigation and residual risks**

The “Identification of Risks” section of this DPIA sets out the inherent risks arising from the proposed data processing. This section summarises the steps to mitigate those risks (which are explained in detail above) and assesses the residual risks, i.e. the level of risk which remains once the mitigations are in place.

Against each risk that have been identified, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Also indicate who has approved the measure and confirm that responsibility and timescales for completion have been integrated back into the project plan.

| **Risk No** | **Risk**  | **Steps to mitigate the risk**  | **DPIA section in which step is described**  | **Effect on risk**Tolerate / Terminate / Treat / Transfer | **Likelihood of harm**Remote / Possible / Probable  | **Severity of harm** Minimal / Significant / Severe | **Residual risk**None / Low / Medium / High |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Personal data may be misused by those with access | 1. External suppliers are on contracts with relevant security and data protection clauses contained within the agreements. Internal security and data protection processes are in place within NHS England.2. All individual users are required to sign security operating procedures that confirm their responsibilities to protect data. Individual Users are also subject to contractual confidentiality requirements. 3. The download functionality of data from the FDP is disabled by default, and access to this is controlled by the relevant FDP User Organisation which ensures appropriate governance in in place. 4. Purpose based access controls are in place to limit access to data. | 1 – section 182 – section 183 – section 184 – section 7 | Treat | Remote | Significant  | Low |
| 2 | Personal data will be processed beyond the appropriate retention period. | 1. Compliance with the Data Security Protection Toolkit (DSPT) requires Records Management policies to be in place.2. Product DPIAs include a section on retention of personal data. | 1 – section 182 – section 15 | Treat | Remote | Minimal | Low |
| 3 | Insufficient organisational measures are in place to ensure appropriate security of the personal data (e.g. policies, procedures, disciplinary controls) |  1.Appropriate organisation measures in relation to data controls and governance are in place to ensure the security of the data.2. Organisational measures are adhered to across the data platform. Any breaches are reported in line with these. | 1 – section 182 – section 4 | Treat | Remote | Significant | Low |
| 4 | Insufficient technical measures are in place to ensure appropriate security of the personal data (e.g. encryption, access controls) | 1. Data is encrypted in storage2. All data to and from the platform is encrypted in transit 3. System level security policies in place to record services compliance to security policy requirements4. Cyber Security Consultancy team assess architecture (including things like threat modelling) to ensure the right technical measures are in place. These include Role Based and Purpose Based Access Controls, effective security monitoring, and encryption in transit and at rest. | 1 – section 42 – section 43 – section 18 | Treat | Remote | Significant | Low |
| 5 | Insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures | 1. An AWS platform configuration review by AWS security team has been performed to ensure that first ingest of data is stored securely.2. Full penetration testing has already been undertaken.3.Regular PEN testing to be scheduled | 1 – sections 4, and 182 – sections 4, and 183 – sections 4, and 18 | Treat | Remote | Significant | Low |
| 6 | Data that has had identifiers removed could be manipulated in some way to re-identify individual people | 1. Access to NHS Data at pseudonymised record level remains in control of the NHS controller. Role Based and Purpose Based Access Controls control who has access to data2. Staff are trained and fully aware of their responsibilities when analysing data to only use the minimum required for their purpose and that it is a criminal offence under the DPA 2018 to knowingly re-identify an individual3. Contracts of employment and other organisational policies provide further safeguards against data misuse4. Product level DPIAs assess the risks of re-identification and identify additional controls that apply at Product level | 1 – section 4 & 72 – section 43 – section 4 | Tolerate | Remote | Significant | Low  |
| 7 | We could lose public trust if our transparency materials are insufficient. This could then lead to a lack of engagement with the NHS and impair health research and planning via an increase in opt-outs. | 1. Transparency achieved through a layered approach, describing various topics at a high level (such as FDP, NHS-PET, National and Local Instances, National and Local Products, etc.), alongside a more detailed FDP Privacy Notices (which also takes a layered approach), and more specific Product Privacy Notices. The FDP IG Framework and DPIAs will also be published to support full transparency.2. Continued engagement with stakeholder and patient groups to support transparency by design and by default and to inform FDP Programme communications to the public.3. Regular FDP Programme Communications to be clear to the public about the approach to the roll out of the FDP f, how FDP works and how privacy is protected, including how NHS-PET works. Be clear about what is current processing and Product and what is future aspirational processing and Product which are not yet agreed to ensure that public is clear on current processing4. Transparency over application of opt outs in high level FDP communications, the FDP Privacy Notice, Product Privacy Notices and Product DPIAs. | 1 – sections 10, and 112 – section 23 – section 114 – section 20 | Treat | Possible  | Minimal | Low |
| 8 | There is a risk that the platform becomes inaccessible to users which could cause delays in the management of patient care and availability of data. | 1. The FDP Contractor is required to have Business Continuity Plans in place to mitigate this risk.2. The relevant FDP User Organisation is required to have Business Continuity Plans in place to mitigate this risk. | Section 4 | Tolerate | Remote | Significant | Low |
| 9 | With data being shared across different organisations and systems, there is an increased risk of data leakage, where sensitive information is inadvertently exposed or shared with unauthorised parties. | Mitigations are in place for organisational measures (risk #3) and technical measures (risk #4). In addition:1. The FDP IG Framework requires that without the appropriate Data Sharing arrangements in place, data cannot be moved between Instances. | Sections 4 and 18 | Treat | Remote | Significant | Low |
| 10 | There is a risk that inadequate data quality process result in errors, inconsistencies and missing information that could compromise the integrity and reliability of the data. | 1. The FDP User Organisation is responsible for the quality of the data being provided to the Data Platform. Where this is Personal Data, there are data protection obligations and DSPT obligations.2. Product DPIAs should consider this risk for individual Products depending on the data sources | Sections 4 and 18 | Tolerate | Remote | Significant | Low |
| 11 | There is a risk that there are inadequate Business Continuity Plans in place to respond effectively to unexpected disruptions such as cyber attacks or downtime. | 1. Under the terms of the contract, the FDP Contractor is obliged to have and maintain Business Continuity Plans.2. FDP User Organisations, as NHS bodies, are obliged to have and maintain Business Continuity Plans. Product DPIAs should consider this risk for individual Products depending on their criticality. | Section 4 | Tolerate | Remote | Significant | Low |
| 12 | There is a risk that users will attempt to access the system from outside the UK, increasing the data security risk. | 1. It is clearly articulated within the FDP IG Framework that no personal/patient data should leave the UK without the express prior approval from the Data Governance Group.2. It is set out in the contract that no access to Personal Data should take place from outside the UK. There are technical controls in place to this effect to prevent access from IP addresses outside of the UK. | Sections 4, 18, and 19 | Treat | Remote | Significant | Low |
| 13. | There is a risk that FDP communications to date may not have fully explained the use of the FDP by NHSE in the national Instance and that individuals were not previously aware of how NHSE and Trusts were processing data in the previous National Data Platform for Products that are now migrating to FDP | 1. Updated communications for the NHSE website have been produced to be clearer about national Instance use, with comms plans to provide more information about FDP and how it is used in the local and national Instances during the Transition Phase
2. The Level 2 FDP Privacy Notice and Level 4 Product Privacy Notices provide full transparency over Processing in Products and will be made available on NHSE website, Local FDP User Organisations have obligations to be transparent and adopt/amend and use these Notices for their local Products
3. Publication in due course of this Overarching DPIA and Product DPIAs will provide more transparency
 | 1 – Section 112 – Section 11 | Tolerate | Possible | Minimal | Low |