Data Protection Impact Assessment for

Falls and Fragility Fracture Audit Programme (FFFAP)

Document control:

	Name and role	Contact details
Document Completed by	**Rosie Dickinson/Lara Amusan**	**rosie.dickinson@rcplondon.ac.uk Lara.amusan@rcplondon.ac.uk**
Data Protection Officer name	**Pamela Forde**	**Pamela.forde@rcplondon.ac.uk**
Document approved by (this should not be the same person that completes the form).	**Teena Chowdhury**	**teena.chowdhury@rcplondon.ac.uk**
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	**Z7085833**	

Date Completed	Version	Summary of changes
9 April 2019	**Draft V0.5**	
12 June 2019	**Draft V 0.7**	**NAIF data breach solution**

Contents

Screening questions

Please complete the following checklist:

	Section	Yes or No	N/A	Comments
1.	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	No		
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		Includes the collection of patient identifiable information. Approval to do this is gained via the section 251 application and approval process.
3.	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where there is an imbalance in the relationship between the position of the individual and the controller.	Yes		FFFAP captures data on all eligible patients through secondary care, which will include the elderly, ethnic minorities and mentally ill patients (the new falls data currently being scoped in 2018 will aim to recruit mental health trusts). Data will only be collected to assess the extent to which the care received meets guidelines and standards and will be fed back to hospitals and commissioners to enable them to improve care.

4.	Does your project involve any innovative use or applying new technological or organisational solutions? This could include biometric or genetic data, the tracking of individuals' location or behaviour?	No		
5.	Does your project match data or combine datasets from different sources?	Yes		Patient identifiers are used to link with HES (for admission and readmission data), ONS (for mortality data) (via NHS Digital).
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	No		Information is gathered from hospitals. Patient information and fair processing information provide details on how and why data is used and what measures are taken to ensure its security.
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	No		
8.	Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project?	Yes		FFFAP has been managed by the Royal College of Physicians for the past 6 years and components of the National Hip Fracture database have been running for over 10 years. A new contract was awarded to the RCP from 1 April 2018 to

				manage the audit for the next 3 to 5 years. The contract includes the review of the previous falls audit which will include a new methodology which will be piloted in 2018.

Data Protection Impact Assessment

This Data Protection Impact Assessment (DPIA) template and guide is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. This tool will help organisations which process personal data to properly consider and address the privacy risk that this entails.

DPIA can be used alongside existing project management and risk management methodologies.

Conducting a DPIA is now a legal requirement under the GDPR (General Data Protection Regulation) which will start on the 25th May 2018 and the new UK Data Protection Act. By completing a DPIA, this will help to ensure that your project is compliant with GDPR and UK data protection legislation. This document will be updated if further ICO guidance is published or there is change in legislation

A DPIA is the basis of a "privacy by design" approach, to help meet privacy and data protection expectations of customers, employees and other stakeholders. A DPIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project.

Purpose and benefits of completing a DPIA

- A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.
- Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.
- The DPIA will help determine the appropriate controls needed to protect personal data i.e. technical, procedural and physical.
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a DPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.
- The ICO may often ask an organisation whether they have carried out a DPIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with Data Protection legislation.

Supplementary guidance

- Data Protection Impact Assessment under GDPR guidance
- ICO's conducting privacy impact assessments code of practice
- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing code of practice may help organisations to identify privacy risks associated with sharing personal data with other organisations.
- The ICO's codes of practice on privacy notices, as well as other more specific guidance, will also help an organisation to focus DPIAs on those issues.
- The Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

DPIA methodology and project information.

At what stage in the project did you conduct this DPIA? E.g. planning stage, changes to the existing project, in retrospect.

This DPIA is being conducted at the beginning of the new FFFAP contract which has been awarded by the HQIP for the next 3 to 5 years. The National Hip Fracture Database (NHFD), Fracture Liaison Service Database (FLS-DB) and National Audit of Inpatient Falls (NAIF) are all continuous audits.

Describe the overall aim of the project and the data processing you carry out

Falls and fractures resulting from falls are major public health problems and thus national priorities for action by the NHS. Better outcomes and secondary prevention are included as measures in the public health, social care and commissioning parts of the NHS Outcomes Framework. The FFFAP consists of three work streams:

- The National Hip Fracture Database (NHFD), a continuous national clinical audit of acute hip fracture care
- The Fracture Liaison Service Database (FLSDB), a continuous national clinical audit of secondary fracture and falls prevention
- The National Audit of Inpatient Falls (NAIF), a continuous clinical audit of falls prevention in hospitals. This work moved from a snapshot audit to a continuous in 2019 and capturing data on falls prevention and post falls interventions for patients with fragility hip fractures

Identifiable secondary care data is entered by local hospitals into a bespoke web-based audit tool provided by Crown Informatics Limited.

For the NHFD and NAIF, Crown Informatics securely transfer identifiable data (NHS number, DOB, Postcode, Name) to NHS Digital to link data and provide appropriate HES and ONS data. For the FLS-DB data linkage is carried on an ad-hoc basis primarily for the purpose of list cleaning (the process for NHFD and FLS-DB is the same).

Linked data is returned to Crown Informatics, which combines the validated identifiers, NHS Digital and the NHFD data. This is then pseudonymised and securely transferred to Oxford University for analysis.

Following the cleaning and analysis data are also transferred from Oxford to the RCP which provides the content for national reports, patient reports, posters and academic papers.

Secondary use of de-identified data for the purpose of audit, service evaluation and research (with appropriate ethical approvals) by approved third parties is also permitted following approval by FFFAP's Scientific & Publications committee at the RCP and HQIP.

Data are release securely from Crown informatics, or if the applicant organisation requires linked data, identifiable data is sent from Crown Informatics to NHS Digital with subsequent flow of a linked (de-identified) dataset from NHS Digital to the applicant organisation.

DPIA Consultation

We advise you to consult with as many relevant people as possible (both internal and external stakeholders**)** while conducting this assessment, consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. Consultation can take place at any point in the DPIA process and may include the project management team, Data Protection Officer, designers, IT provider, procurement team, data processors, communications team, patients, stakeholders, corporate governance and compliance teams, researchers, analysts, statisticians and senior management.

You must consult with the Data Protection Officer regarding the impacts on privacy. Please state below that you have.

If you decide against seeking the views of data subjects or their representatives e.g. this would be disproportionate or impracticable, then the justification must be made clear in the box below.

In the box below name the stakeholder group, date consulted and how consulted. Please insert another box if you consulted with many different stakeholder groups.

RCP Data Protection Officer, Operations director of Audit and Accreditation department at RCP, sub-contractors for webtool and analysis, RCP IT.

Publishing your DPIA report

Publishing a DPIA report is not a legal requirement but you should consider publishing this report (or a summary or a conclusion) and you should send it to your stakeholders. Publishing the DPIA report will improve transparency and accountability, and lets individuals know more about how your project affects them. Though there may be a need to redact/remove sensitive elements e.g. information on security measures.

State in the box below if you are going to publish your DPIA. If so, please provide hyperlink to the relevant webpage if this has been done already or insert the date you intend to publish it.

This DPIA has been published on our website: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements

Data Information Flows

Please describe how personal information is collected, stored, used and deleted. Use your data flow map and information asset register to help complete this section. Explain what personal information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. Completing this section can help identify potential 'function creep', unforeseen or unintended uses of the data for example data sharing.

FFFAP have three data flow maps for the audit workstreams attached as appendices:

- NHFD (appendix A)
- FLS-DB (appendix B)
- NAIF (appendix C)

They also refer to information on the contact details we hold for audit participant and FFFAP staff contracts.

The FFFAP information asset register is included in appendix D.

Transferring personal data outside the European Economic Area (EEA)

If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries, or how the data is adequately protected).

No personal data are transferred outside of the EEA.

Justification for collecting personal data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. In certain circumstances it may be unlawful to process information not described in the transparency information (privacy notice/fair processing material) which informs individuals how their personal data is being used.

It may not be necessary to process certain data items to achieve the purpose. They may be irrelevant or excessive leading to risk of non-compliance with the Data Protection Act.

In the tables below list and justify personal data items needed to achieve the lawful aim of a project that requires information on individuals and their personal characteristics. Insert as many more lines that you need. Work through the table of items and decide whether or not you should be collecting the information, examine each data field and decide if you need it.

There are two sections in the table below, one for personal data and one for personal sensitive data items.

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	Y		For NHFD and NAIF: Patient's Name: To assist linkages at MRIS/NHSCR where no NHS Number is provided or the number is incorrect patients name is required for tracing at MRIS. Name is not needed for analysis and is retained only until the NHS number is traced via MRIS, we then have no reason to keep this data item. Contact list for audit participants, FFFAP newsletter distribution and inviting to events/workshops.
Address	Y		For NHFD and NAIF: Postcode of usual address: The address at date of diagnosis is used to enable analysis by locality of patients [postcode]. Full postcode is crucial for MRIS list cleaning purposes, to allow us to link to mortality data and to discover missing NHS Numbers. Derived data are used for analysis, such as age, CCG, deprivation. Postcode is not needed for analysis and is retained only until the NHS number is traced via MRIS and/or deprivation codes have been calculated, we then have no reason to keep this data item
Postcode	Y		FOR NHFD and NAIF: As above

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
DOB	Y		For NHFD and NAIF: Birth Date: To enable age at diagnosis to be established for epidemiological and survival analysis. To enable analysis by birth cohort and to assist linkage at MRIS/NHSCR [date of birth. Date of birth is crucial for MRIS list cleaning purposes, to allow us to link to mortality data and to discover missing NHS Numbers. DOB is not needed for analysis and is retained only until the NHS number is traced via MRIS and/or age at event is calculated, we then have no reason to keep this data item
Age	N		
Sex	Y		This contributes to the case mix adjustment model for NHFD and FLS-DB.
Marital Status	N		
Gender	N		See sex
Living Habits	N		
Professional Training / Awards	N		
Income / Financial / Tax Situation	N		
Email Address	N		
Physical Description	N		
General Identifier e.g. NHS No	Y		As above
Home Phone Number	N		
Online Identifier e.g. IP Address/Event Logs	N		
Website Cookies	N		
Mobile Phone / Device No	N		
Device Mobile Phone / Device IMEI No	N		
Location Data (Travel / GPS / GSM Data)	N		
Device MAC Address (Wireless Network Interface)	N		
Sensitive Personal Data			
Physical / Mental Health or Condition	N		
Sexual Life / Orientation	N		

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Family / Lifestyle / Social Circumstance	N		
Offences Committed / Alleged to have Committed	N		
Criminal Proceedings / Outcomes / Sentence	N		
Education / Professional Training	N		
Employment / Career History	N		
Financial Affairs	N		
Religion or Other Beliefs	N		
Trade Union membership	N		
Racial / Ethnic Origin	N		
Biometric Data (Fingerprints / Facial Recognition)	N		
Genetic Data	N		
Spare			
Spare			
Spare			

Data quality standards for personal data

In the box below, describe how you will ensure that personal data is accurate and kept up to date.

Streamlining of datasets will help minimise data entry omissions. Comprehensive validation rules are built into the web-tool to ensure that incorrect, conflicting and/or illogical data cannot be saved.

Comprehensive guidance and help notes for NHFD, NAIF and FLS-DB are provided online and the questions are reviewed annually by the board and advisory groups in order to ensure they are necessary for the core purpose of the audits. Crown Informatics and FFFAP Team operate a helpdesk to answer queries from participants submitting data.

The FFFAP team, including clinical leads, work with specialist societies and opinion leaders to encourage the local collection of high quality data.

The audit has a minimum duty to hold data on a five year retention period, but data processors have a duty to hand over the data to any subsequent processor or data owner when they are no longer authorised/out of contract to hold that data.

To maintain up to date contact details Crown Informatics encourage users themselves, user department colleagues, and RCP administrators/helpdesk to inform them of leavers and accounts to be suspended. To back this up, they annually run 'dormant user purges' to remove unused and unconfirmed accounts.

Individual's rights

If your project uses personal data you must complete this section.

If your project uses personal data you must state how fairness and transparency will be achieved e.g. privacy notices on websites, posters, and leaflets. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to children should be in such a clear and plain language that the child / vulnerable person can easily understand.

In the box below, please define the way you have ensured that individuals are aware of the rights, if they request those rights how will they achieve them? For example if an individual requests a copy of their information held by you, describe how you would do this. You can insert any relevant policy or process guides in the appendix at the end of this document if they are not already available on your website. This section does not refer to the personal information held about your audit staff.

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
Individuals are clear about how their personal data is being used.	Fair processing notices are available for NHFD, NAIF and FLS-DB Patient information leaflets are made available to ensure patients are aware of their data being used and for what purpose.	For FLS-DB information is available online and in a patient booklet: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements For NHFD information is available online and made available in PDF form for Trusts to print: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements NHFD Patient info leaflet v7.0 2018.pdf For NAIF information is available online and in a patient booklet: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements	**Information from the FLS webpages:** **Why do you need this personal information?** To know whether an FLS has successfully prevented you from suffering a second fragility fracture we need to be able to look at your care over a period of time and possibly across different geographical locations. If you did suffer a second fracture, it might not happen for months or years after your first fracture. You might have moved house, or you might be on holiday in a different area of the country. Collecting this information allows us to link to other national data sets which provide further information about patient care and outcomes of care. For example, if you started treatment at one FLS and then moved to an area that did not have an FLS, we could still identify any treatment you received in your new location and find out how successful your fracture prevention treatment was. If we did not collect confidential information we would not get accurate information on the quality of

			your care.
Individuals can access information held about them			Will uphold right to access.
Request erasure (right to be forgotten) in certain circumstances, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes	All fair processing information and patient information leaflets provide individuals with the right to have their information removed from or not included in the audit. The section in the patient information is called 'Say no thank you'.	For FLS-DB information is available online and in a patient booklet: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements For NHFD information is available online and made available in PDF form for Trusts to print: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements  NHFD Patient info leaflet v7.0 2018.pdf For NAIF information is available online and in a patient booklet: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements	Saying 'no thanks' National clinical audit works best when it includes information from as many patients as possible. If you do not want your information to be used then please tell the people who are treating you. Your doctor or nurse will be able to note that you do not want to participate and your data will not be used. If you change your mind and want to arrange for your data to be removed please call, email or write to: Crown Informatics Limited Enterprise Centre Randall Way Retford Nottinghamshire DN22 7GR Email: enq@crowninformatics.com Tel: +44 (0)1777 709009. Not taking part in the audit will not affect your treatment in any way.
Rectification of inaccurate information	N/A	N/A	See section on Data quality standards for personal data
Restriction of some processing			Guidance here from HQIP needed: restriction, objection, withdrawal beyond point of collection will impact on validity of FFFAP
Object to processing undertaken on some legal bases			As above
Complain to the Information Commissioner's Office;	No	No	Information will be available on updated Fair Processing Statements
Withdraw consent at any time (if	N/A s251 in place for FFFAP		*As processing.*

processing is based on consent)			
Data portability (if relevant)	N/A	N/A	N/A
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	This information is given within all fair processing notices.	Fair processing notices are available for FLS-DB, NAIF and NHFD	Example: Who runs the FLS-DB? The data controller – who has overall responsibility for the collection, storage and processing of personal identifiable information – is the Healthcare Quality Improvement Partnership (HQIP). However, HQIP will not be processing any of the data. The FLS-DB is managed by the RCP on behalf of HQIP as part of the Falls and Fragility Fracture Audit Programme (FFFAP). This is a multidisciplinary national clinical audit which is being carried out in partnership with a number of organisations: •British Orthopaedic Association •British Geriatrics Society •Royal Osteoporosis Society •Public Health England. The University of Oxford will be analysing the data for the results.
In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will protected (e.g. the recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.	N/A	N/A	N/A
To know the legal basis under which their information is processed. Is there a clear legal basis for the processing of personal data? If	This information can be found in both the fair processing notices		

so, what is the legal basis?			
To know the purpose(s) for the processing of their information.	The fair processing notices and patient information leaflets and online webpages include information on this.		FLS example: How will my confidential information be used? Crown Informatics will periodically send data to NHS Digital, who link the records to the Office for National Statistics (ONS) and get details of your registered GP practice via a process known as 'list cleaning'. In order to link the data, we need to provide identifiable data (NHS number and date of birth) to NHS Digital; we will receive back information containing your GP practice code. This will allow us to link the patient data to a CCG and report at CCG level. By linking the data together, we are able to look at more aspects of quality of care without asking hospitals to enter more information into our database. Data is supplied to the University of Oxford for analysis but this will be done so that no individual patient can be identified. Reports produced by the audit will not contain NHS numbers or any other information that could be used to identify anyone. We sometimes get requests from hospitals, universities, and academic or healthcare organisations who want to carry out research using the data that we collect. We always ensure that researchers that we agree to share data with have appropriate legal approvals in place to share data and we will never release information that could be used to identify you as an individual.
Whether the provision of personal data is part of a statutory obligation and possible consequences of	N/A	N/A	N/A

failing to provide the personal data.			
The source of the data (where the data were not collected from the data subject)	Fair processing statements		Example of FLS: Breaking a bone after a fall is a common injury and caring for patients with these broken bones or fractures, and preventing future fractures, is an important part of the work of the NHS. **This hospital takes part in the FLS-DB**, which has been set up to improve the care of patients who are at risk of a fragility fracture or osteoporosis.
Categories of data being processed	Datasets and data flows.	Audit datasets and data flows are available online	For FLS: What information do you collect? The FLS-DB will collect information about the care you are given by an FLS if you are at risk of a second fragility fracture or of osteoporosis. In order to monitor standards of care we need to collect the following personal information: •NHS number (a unique number) •date of birth •postcode.
Recipients or categories of recipients			Example from FLS- DB: Crown Informatics will periodically send data to NHS Digital, who link the records to the Office for National Statistics (ONS) and get details of your registered GP practice via a process known as 'list cleaning'. In order to link the data, we need to provide identifiable data (NHS number and date of birth) to NHS Digital; we will receive back information containing your GP practice code. This will allow us to link the patient data to a CCG and report at CCG level. By linking the data together, we are able to look at more aspects of quality of care without asking hospitals to enter more information into our database.

			Data is supplied to the University of Oxford for analysis but this will be done so that no individual patient can be identified. Reports produced by the audit will not contain NHS numbers or any other information that could be used to identify anyone. We sometimes get requests from hospitals, universities, and academic or healthcare organisations who want to carry out research using the data that we collect. We always ensure that researchers that we agree to share data with have appropriate legal approvals in place to share data and we will never release information that could be used to identify you as an individual.
The source of the personal data	The patient information leaflets, online information and fair processing statements provide this information.	For FLS: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements For NHFD: information is available online and made available in PDF form for Trusts to print: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements  NHFD Patient info leaflet v7.0 2018.pdf For NAIF information is available online and in a patient booklet: https://www.rcplondon.ac.uk/projects/outputs/fffap-data-processing-statements	Example: What does it mean to be a part of the FLS- DB? Being part of the FLS-DB does not mean that you will be given different care or have your treatment options limited. The FLS-DB will just collect the details of what type of care you receive in order to understand how the FLS in your area identifies patients, investigates their individual circumstances, provides information to you and refers you to treatment if necessary. By collecting this information the FLS-DB can help the NHS understand how care is being implemented across the country and make sure that all patients are getting the best possible care.
To know the period for which their data will be stored (or	The patient information leaflets, online information and fair	FLS-DB, NAIF and NHFD fair processing information	Example from FLS-DB: Where does my confidential

the criteria used to determine that period)	processing statements provide this information.		information go? The FLS-DB has a legal duty to protect your information and maintain confidentiality. Your information will be held safely on a secure computer database by our experienced IT team at Crown Informatics, who follow best practice in data protection and security. The data collected are subject to strict rules about confidentiality including those of the Data Protection Act (1998), the Health and Social Care Act (2001) and to the recommendations of the Caldicott Report (1997). **It will be held for the duration of the audit. Should the audit come to an end, it will be held for a further 5 years after that.** Staff at Crown Informatics are all fully trained in information governance and will only see personal details for database administration and have to follow strict confidentiality rules.
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	N/A	N/A	N/A

Privacy Risks

Types of Privacy risks

- Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organisation), for example; failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regards to the individual's privacy.

In the box below insert the number of individuals likely to be affected by the project. This could be the number of unique patient records your project holds now and how many more records you anticipate receiving each year.

NHFD
There are currently just over 500,000 NHFD clinical records on the webtool.

Cohort size for 2018 will be approximately 80,000 patients.
Predicted cohort size- increase by 2-3% per annum – therefore
2019- 81,600
2020- 83,200
2021- 84,800

FLS-DB
The number of FLSs is not constant and as more are commissioned or decommissioned the number of patients will change – approx.:

2018 – 40,000
2019 – 40,400
2020 – 40,800
2021 – 41,200

NAIF
Although new methodology not yet established, we estimate the cohort size to be:
2018 – not collecting data
2019 – 2,200
2020 – 2,244
2021 - 2,288

Please complete the table below with all the potential risks to the Individuals of the information you hold on them, your corporate risks and compliance risks.

When completing the table you need to consider if:

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- 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.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate and compliance risks

In the table, list the corporate risks to your organisation which could include reputational damage, loss of public trust, financial costs and data breaches. Below these, insert any compliance risks.

Possible corporate risks include:

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

Examples of compliance risks include:

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the GDPR.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Managing Privacy and Related risks

There are many different steps you can take to reduce a privacy risk. For example

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.

- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Use your project plan and a detailed explanation of information flows to identify more precisely how a general risk may occur. For example, there may be particular points in a process where accidental disclosure is more likely to happen.

The DPIA actions should be added to into your project plan and risks added to your contract review documentation.

Privacy Risks and Actions Table

Please see appendix 2 for additional guidance on completing this table

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 -Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk OR Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Illegitimate access to information For NHFD & NAIF – NHFD database users entering incorrect hospital name of inpatient fall location, resulting in NAIF database users incorrectly receiving identifiable data.	3	3	9	**Reduced**	Crown Informatics Ltd holds all identifiable information on behalf of FFFAP. The FFFAP team and Oxford only have access to pseudo-anonymised data. **Data security at Crown** (web-tool in use for secondary care). Only nominated individuals at each hospital have access to the data, and only the individual units themselves can see the PIDs of their own patients. Access to data is via secure client software, operating over secure VPN firewalled	Crown ensures that all data is held safely and the risk of breach is an absolute minimum. **Once the mis assigned record is rejected, it is deleted from the NAIF system so identifiable data cannot be accessed in the NAIF database.**	July 2019	Program me manager

					networks using secondary application layer security provided by IBM. Data is stored and processed at a secure data centre; this operates to ISO 27001 certification (2015). Any users that have access to identifiable data have to be registered with Crown and have login details to a secure webtool **An extra option has been added for users to refuse mis-assigned records and delete them which sends an email to the initial user entering the patient on the NHFD requesting the record to be reassigned correctly.**			
Undesired modification	1	4	4	**Reduced**	As above	As above		
Disappearance of data	1	3	3	**Reduced**	Crown Informatics Ltd Backups are encrypted at AES256, held in dual copies, and stored securely.	Crown ensure that all data is held safely and the risk of disappearance or loss of information is at an absolute minimum.		
Network failure (RCP)	1	5	5	**Reduced**	Data security at RCP. Data is regularly backed up on a server, and access to both servers are certified to ISA 7001. This will ensure that despite a	This ensures that even if a network failure is experienced all information remains safe and		

					network failure access can still be gained to key information.	unharmed.		
Sub-contractor network failure or cyber-attack	2	5	10	**Reduced**	Crown Informatics Ltd holds all identifiable information on behalf of FFFAP. The FFFAP team and all other sub-contractors do not have access to this. Data security at Crown (web-tool in use for secondary care). Only nominated individuals have access to the data, and only the individual units themselves can see the PIDs of their own patients. Access to data is via secure client software, operating over secure VPN firewalled networks using secondary application layer security provided by IBM. Data is stored and processed at a secure data centre; this operates to ISO 27001 certification (2015). Backups are encrypted at AES256, held in dual copies, and stored securely. Oxford NDORMS information security	Crown security systems ensure that all data is held safely and the risk of breach is an absolute minimum. All the necessary fire walls and precautions are in place to deal with and avoid with cyber events.		

					policy is listed below Oxford NDORMS Information Security I			
Data breach: The audit programme would have a complex range of data flows, dependent on several external providers and technical systems. If any of these fail or an error is encountered, and data breach occurs - this would be exceptionally serious for the audit programme's reputation, budget, ability to function, and to guarantee patient confidentiality.	1	5	6	**Reduced**	The audit programme is subject to comprehensive data regulations, and will do the following to both reduce and transfer the risk of a data breach: - Legal basis. FFFAP has a s251 in place. - Data security at Crown Only nominated individuals have access to the data, and only the individual units themselves can see the PIDs of their own patients. Access to data is via secure client software, operating over secure VPN firewalled networks using secondary application layer security provided by IBM. Data is stored and processed at a secure data centre; this operates to ISO 27001			

					certification (2015). Backups are encrypted at AES256, held in dual copies, and stored securely. - Data security at RCP and ICL. Data is regularly backed up on a server, and access to both servers are certified to ISA 7001, the recognised standard for data security. NDORMS operates with two core information security documents. These are a management policy and practical guidelines: NDORMS Information Security Guidelines : All new members of the department, including students and visitors, are provided a face-to-face information security induction. Members of NDORMS are required to complete annual training to ensure their			

					understanding stays up to date. The Big Health Data Research group deals with large volumes of sensitive data and has maintained NHS Information Governance Toolkit certification since 2015 to give assurance to data providers. It works within information governance policies for the whole department along with additional controls. https://www.ndorms.ox.ac.uk/information-security-policy - All members of the audit team have data protection training on an annual basis. Posters, patient information leaflets and fair processing information are made widely available to ensure that patients are aware of the audit and how and why their data is used.			

					There is the option for them to ask for their information not to be included in the audit if they do not wish it to be. **If a patient asks to be** removed they are completely removed from the live database(s), subject to clear instructions and identity checks, but not backup databases. Where a patient record has been de-identified, that data cannot be removed. Access to backups is strictly encrypted and controlled.			
Corporate risks & compliance risks section								
National Data Opt-out risk	2	3	5	**Accepted**	There is a risk that patients who have opted-out of having their patient identifiable information used for audit/research/planning purposes will be incorrectly entered onto the audit webtool. Responsibility for not entering that patients			

					data is solely with the hospital/health and social care service who are entering the data. This has been put as a 2 as with the introduction of this on 25 May 2018, this is a very new process and issues cannot be pre-empted at this point.			
Section 251/legal basis annual reviews – not submitted	1	4	4	**Reduce**	The legal basis requirements involve an annual review of the section 251. There is a risk that these are delayed or not submitted and FFFAPs legal basis is not valid for a time period. All senior programme staff (clinical leads, programme and project managers) are to have an awareness of these process and the dates that they are due. Reminders are placed in calendars and in project plans to ensure all necessary teams members are aware of the requirement to update these essential documents and approvals.	With all senior team members knowing the details and dates of these that the likelihood of them being missed is significantly reduced.		

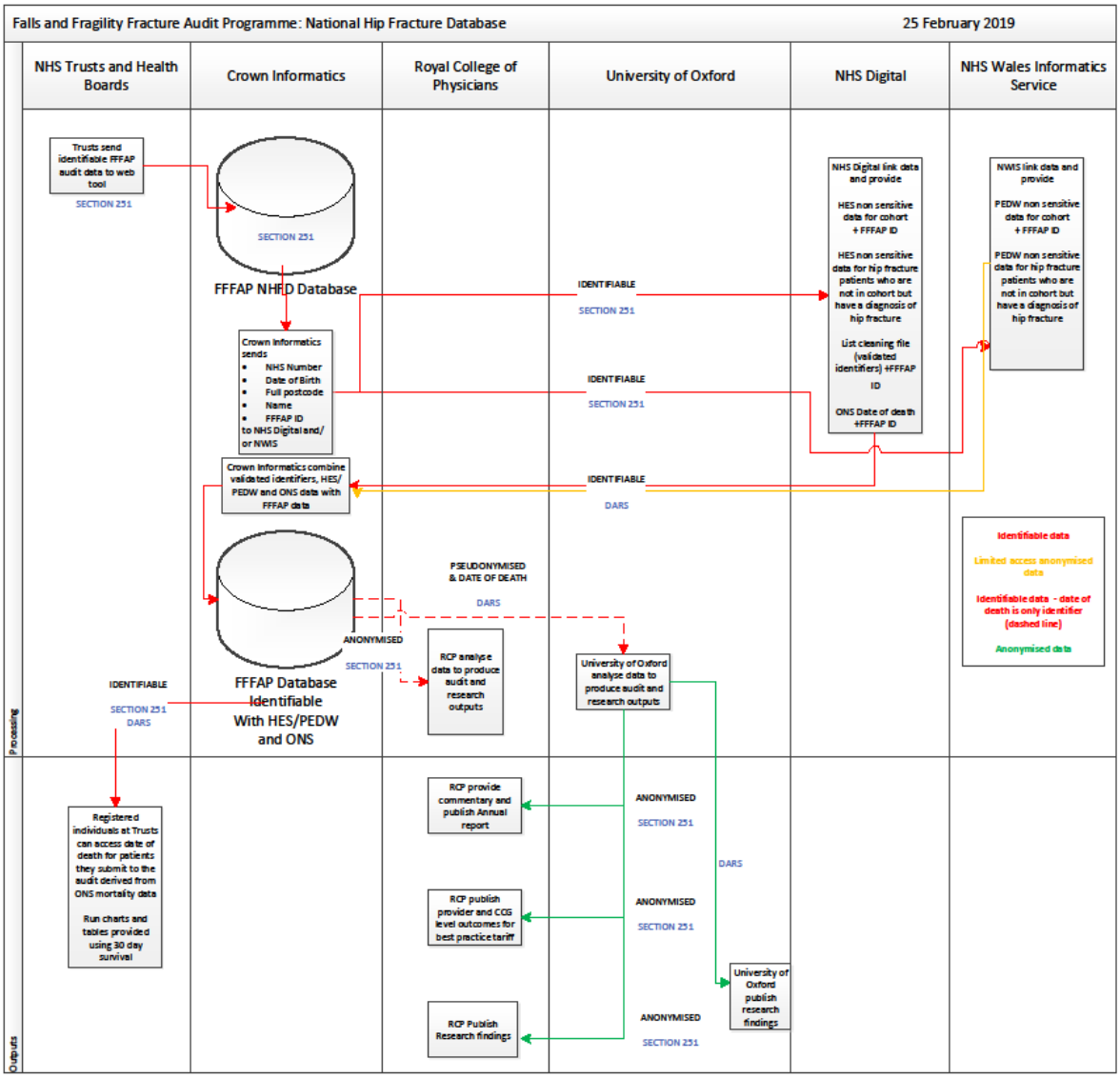
Regularly reviewing the DPIA

DPIA should be an ongoing process and regularly reviewed during the lifecycle of the project or programme to ensure

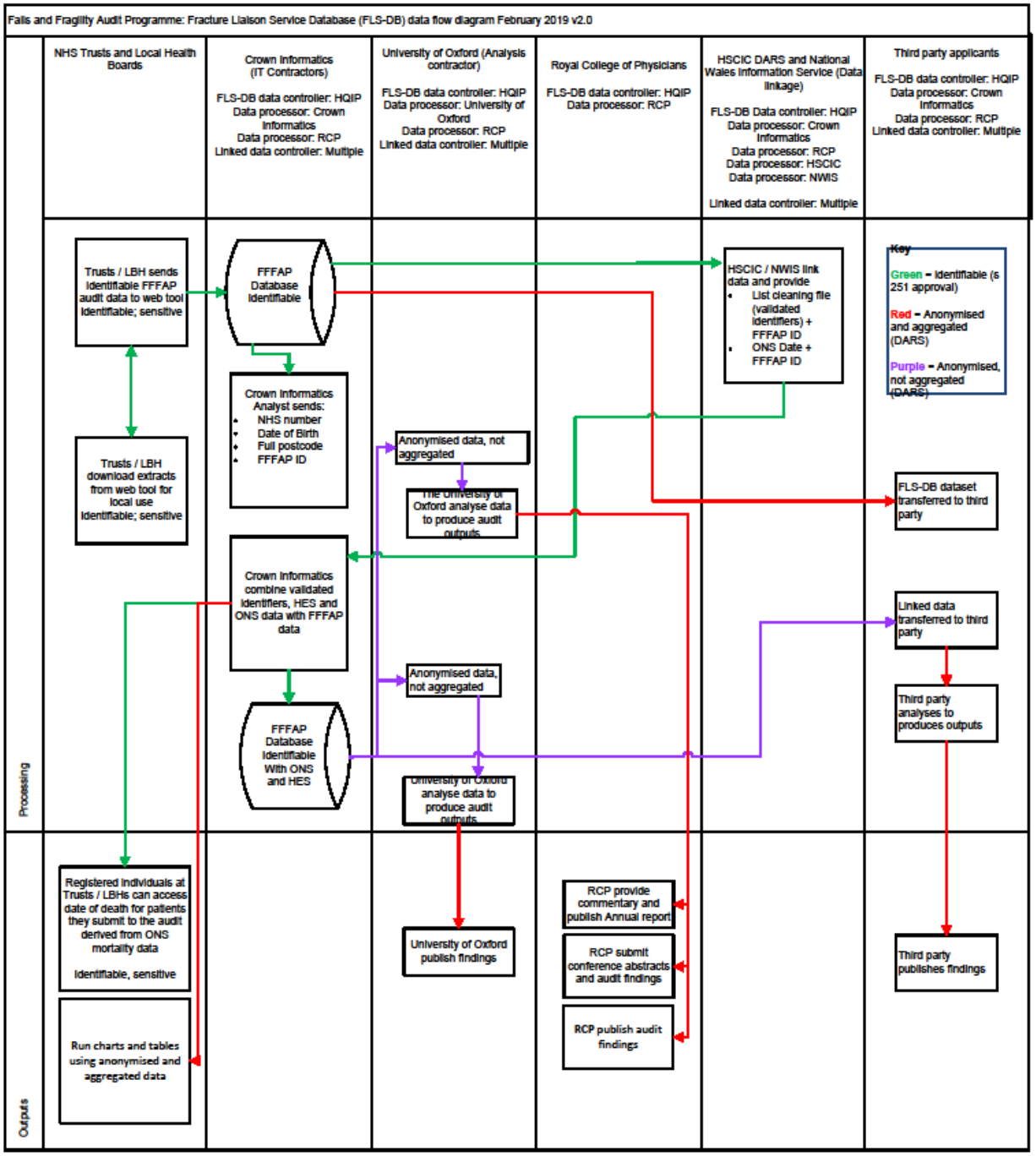
- Risks identified are still relevant
- Actions recommended to mitigate the risks have been implemented and mitigating actions are successful

You must add to your DPIA every time you make changes to the existing projects, send an updated version to your HQIP project manager and ensure that you incorporate any identified risks/issues to your risk/issue registers of the project contract review form.

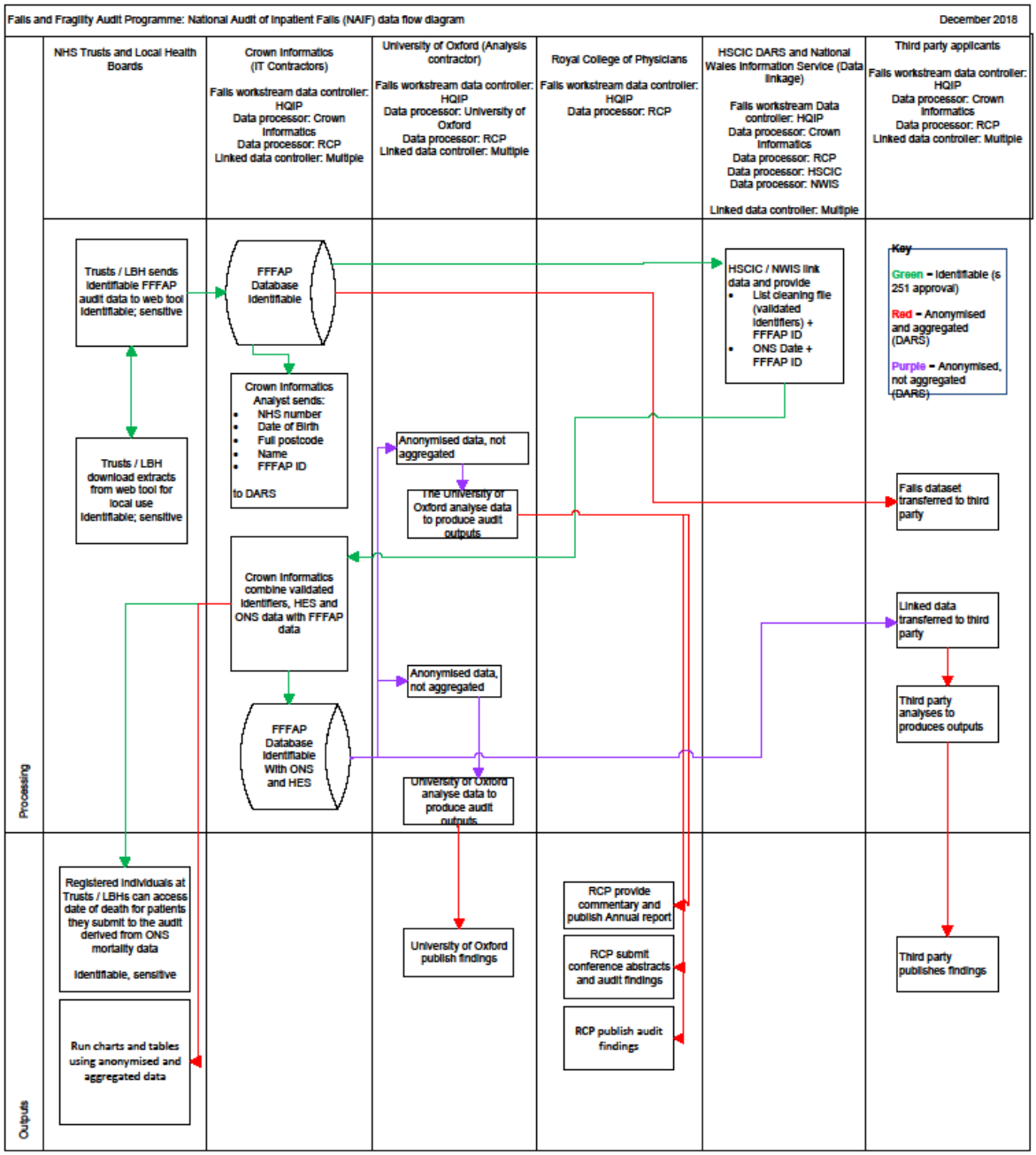
Appendix A NHFD data flow



Appendix B FLS-DB data flow



Appendix C NAIF data flow



Appendix 1 Submitting your own version of DPIA

If submitting your own version of DPIA please ensure it includes the following items. If any items are missing please add this to your DPIA and then submit it. You must also complete the screening questions above.

	Checkbox – Please tick	Evidence – Page number and section in your DPIA
Confirmation of advice /consultation sought from Data Protection Officer whilst completing the DPIA		
Name of DPO		
Name and role of person approving completion of DPIA form. This must not be the same person that completes the form.		
Will the DPIA be published or part of it such as the summary or conclusion (not essential but encouraged). If so, where is it published?		
Does it include a systematic description of the proposed processing operation and its purpose?		
Does it include the nature, scope, context and purposes of the processing		
Does it include personal data, recipients and period for which the personal data will be stored are recorded		
Does it include the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)		
Does the DPIA explain how each individual's rights are Managed? See section on individuals rights		
Are safeguards in place surrounding international transfer? See section on sending information outside the EEA		
Was consultation of the document carried out and with whom?		

Organisations ICO registration number		
Organisations ICO registration expiry date		
Version number of the DPIA you are submitting		
Date completed		

Appendix 2 Guidance for completing the table

<table>
<tr><td>What are the potential risks to the individuals whose personal data you hold?</td><td>See examples above</td></tr>
<tr><td>Likelihood of this happening (H,M,L)</td><td>
<table>
<tr><th>Likelihood score</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Very unlikely</td><td>May only occur in exceptional circumstances</td></tr>
<tr><td>2</td><td>Unlikely</td><td>Could occur at some time but unlikely</td></tr>
<tr><td>3</td><td>Possible</td><td>May occur at some time</td></tr>
<tr><td>4</td><td>Likely</td><td>Will probably occur / re-occur at some point</td></tr>
<tr><td>5</td><td>Very likely</td><td>Almost certain to occur / re-occur</td></tr>
</table>
</td></tr>
<tr><td>Impact (H,M,L)</td><td>
<table>
<tr><th>Impact scores</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Insignificant</td><td>No financial loss; disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality</td></tr>
<tr><td>2</td><td>Minor</td><td>Minor (<£100k) financial loss / disruption to systems; procedures require review but manageable; limited slippage in work activity, breach of confidentiality where < 20 records affected or risk assessed as low where data pseudonymised/files encrypted and no sensitive data</td></tr>
<tr><td>3</td><td>Moderate</td><td>Disruption to financial systems (<£250k); significant slippage in work activity or resources e.g. delay in recruiting staff; procedures and protocols require significant review, breach of confidentiality/ loss personal data where < 100 records involved and no sensitive data</td></tr>
<tr><td>4</td><td>Major</td><td>Major financial loss (£500k); large scale disruption to deliverables & project plans; business activity severely undermined, wasting considerable time / resources; poor quality report leading to loss of confidence in provider / HQIP / NHSE, breach of confidentiality/loss of personal sensitive data or up to 1000 records</td></tr>
</table>
</td></tr>
</table>

	5	Catastrophic	Huge financial loss (>£500k); significant threat to viability of the organisation in total or in part; huge disruption to business activity; almost total lack of confidence in project provider / HQIP / NHSE, serious breach of confidentiality/loss of personal sensitive data >1000 records involved
Risk score (calculated field)	Please multiply the likelihood by the severity (likelihood x severity = risk score). This score will help to rank the risk so the most severe risks are addressed first		
Will risk be accepted, reduced or eliminated? (where risk is accepted give justification)	A = Accepted (must give rationale/justification) R = Reduced E = Eliminated		
Mitigating action to reduce or eliminate each risk	Insert here any proposed solutions – see managing privacy and related risks section above OR If a risk has been accepted please give justification here (The purpose of the DPIA is to reduce the risk impact to an acceptable level while still allowing a useful project to be implemented.)		
Explain how this action eliminates or reduces the risk	Describe how your proposed action eliminates or reduces the possible risk. You may want to assess the costs/resource requirements (i.e. purchasing additional software to give greater control over data access and retention) and balance these against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.		
Expected completion date	What is the expected completion date for your proposed action? Ensure that DPIA actions are integrated into the project plan. You should continue to use the PIA throughout the project lifecycle when appropriate. The DPIA should be referred to if the project is reviewed or expanded in the future.		
Action Owner	Who is responsible for this action?		