Data Protection Impact Assessment
Falls and Fragility Fracture Audit Programme

DPIA completion and review process

A DPIA needs to be undertaken/updated:

1. When the project contract is procured/reprocured:
    a. Completed by the project provider once the contract is in place and before the data processing starts
    b. Reviewed and signed off by HQIP's CEO

2. When the project contract is extended:
    a. Completed by the project provider and submitted once the extension is in place
    b. The project AD should be checking this is completed in their contract review meetings as it is one of the contract deliverables

3. When the project contract is varied:
    a. Completed by the project provider before the change to the data processing takes place
    b. Reviewed by HQIP's IG Lead/DPO and signed off by HQIP's CEO.

4. Where any new changes to the processing of data are planned to be introduced into the project and before the implementation of such changes:
    a. For instance:
        i. Changes to data flows or data items
        ii. Where new data linkage is planned
        iii. Where new technology is planned which affects the processing of the project data
        iv. Where the project section 251 CAG approval is being amended
    b. In these instances, a DPIA needs to be completed by the project provider where processing is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use the **Screening checklist** below to help you decide when to do a DPIA
    c. Reviewed by HQIP's IG Lead/DPO and signed off by HQIP's CEO

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 need to incorporate any identified risks/issues to your risk/issue registers of the project contract review form.

All project specific DPIAs are reviewed **annually** by HQIP's DPO as part of the annual IG Checklist review in Podio.

Screening checklist

Please complete the following checklist. Answering **one or more** of the Screening questions with a 'Yes' would require completion of DPIA for the proposed processing activity:

No.	Screening questions	Yes / No	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 managed by the Confidentiality Advisory Group (CAG) on behalf of the Secretary of State for Health.
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 National Audit of Inpatient Falls also collects data from specialist, community and 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), Civil Registration Data

			(for mortality data via NHS England).
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. We also have national data opt out information for projects depending on whether the project is exempt from opt out or not.
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?	No	FFFAP has been managed by the Royal College of Physicians (RCP) since 2013 and components of the National Hip Fracture Database have been running since 2007. The programme has been successful in securing a new contract starting July 2023 for an initial period of 3 years. All three audits (National Hip Fracture Database; National Audit of Inpatient Falls and Fracture Liaison Service Database) are continuous.

Stage 1. Identify the need for a DPIA

*Set out the outcomes and reasons identified in your screening assessment, or as may be expected by HQIP (see the list of circumstances in **DPIA Completion and review process** above) here to explain why you have concluded a DPIA is necessary*

Screening assessment outcome:
DPIA required as three screening questions answers are 'yes'.

Reason for completing the DPIA:
Updating DPIA to the new form as part of the annual review of the DPIA, to ensure:

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

Stage 2. Consultation

Who are the people involved in the processing or affected by it?

- *Individuals*
- *Data processors (third parties who process the data on behalf of the organisation)*

Sub-contractors for webtool (data processors), Sub-contractors for data analysis, patients, clinical staff, hospital administrators.

Who will you consult? When will you consult them? How will you consult them?

- *The organisation's Information Governance team*
- *HQIP's project manager*
- *HQIP's DPO*

RCP Data Protection Officer, Operations director of Care Quality Improvement Directorate at RCP, sub-contractors for webtool (data processors) and analysis teams will be involved in compiling the information included. Our patient and carer panel review our outputs and will be reviewing our fair processing statements, the length of the DPIA and level of detail was felt impractical to request a review. The fair processing statements contain the relevant data processing information in a more accessible format. We are also producing lay friendly posters summarising our fair processing information for hospitals to use in patient facing settings.

If you do not intend to consult any or all of the people you have identified, why not?

n/a

Stage 3: Data processing

Part 1: Describe the purpose of the processing

What will the data be used for?
What do you want to achieve by processing the data?

What benefit is there to the processing for:

- *You?*
- *The individuals?*
- *The wider public?*

Falls and fractures are a major public health problem 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 hip and femoral 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 audit in 2019 and captures data on falls prevention and post falls interventions for patients with fragility hip and femoral fractures

Identifiable secondary care data is entered by hospital staff into a bespoke web-based audit tool provided by Crown Informatics Limited.
For the NHFD, Crown Informatics securely transfer identifiable data (NHS number, DOB, Postcode, Name) to NHS England to link data and provide appropriate HES and Civil Registration data.
Linked data is returned to Crown Informatics, which combines the validated identifiers, NHS England and the NHFD data. This is then pseudonymised and securely transferred to University of Bristol for analysis. Following the cleaning and analysis aggregated and anonymised data are also transferred from Bristol 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 Access Review Group (DARG). Data are released securely from Crown informatics, or if the applicant requires linked data, identifiable data is sent from Crown Informatics to NHS England with subsequent flow of a linked (de-identified) dataset from NHS England to the applicant organisation.

Part 2: Insert a data flow diagram

- *Outline the data processing locations*
- *Include information about the methods used for transferring the data from one location to another (e.g., encrypted file with password sent separately, secure electronic transfer, etc)*
- *If an existing project, please highlight any changes made to the current data flow (e.g., new data linkage, new processing location, new method of data transfer, etc)*

FFFAP have three data flow maps for the audit workstreams:

- NHFD
- FLS-DB
- NAIF

All data flows available: https://www.rcp.ac.uk/improving-care/national-clinical-audits/falls-and-fragility-fracture-audit-programme-fffap/fffap-data-processing-statements/

Data collection: Local sites (i.e. clinicians, members of the audit team) enter audit data (including patient identifiable data – PID) for appropriate patients via a bespoke web-tool hosted by Crown Informatics (www.fffap.org.uk).
Linkage: Crown sends identifiable data to NHS England for linkage purposes and FFFAP data is combined with HES and Civil Registration Data. All linked data is returned to Crown.
For NHFD: Crown will combine the validated identifiers, NHS England and the FFFAP data. Crown anonymises data (audit and linked). Specifically, date of birth transformed to age and date of death is transformed into 30-day mortality. **For NAIF: prior to 2025 NAIF data is linked with originating case in NHFD.** Crown will combine the validated identifiers, NHS England and the FFFAP data. Crown anonymises data (audit and linked). Specifically, date of birth transformed to age and date of death is transformed into 30-day mortality. After 2025 NAIF is a stand alone audit and will not have linkages.
Data analysis and management: Pseudonymised patient level audit data is sent to University of Bristol for data cleaning and analysis. Following the cleaning and analysis of data, aggregated (i.e. analysed and non-identifiable) data will be transferred from University of Bristol to the RCP to provide commentary for, and then publication on, outcome-related audit programme outputs (e.g. national, trust and health board level reports).

Part 3: Describe the processing that will take place

- *What data will be collected?*
- *Will special category data be collected? If yes, what categories of data will be collected?*
- *Whose data will be collected?*
- *Are any of the individuals whose data is being collected children or vulnerable groups of people?*
- *How will the data be collected? (Include details of the means of collection e.g., directly from individual/face to face or indirectly)*
- *What is the geographical area that will be covered?*
- *How often will the data be collected?*
- *Will the data be shared with a third party? If yes then name them here.*
- *If sharing data then have you entered into a data sharing or data processing agreement with them? If not, why not.*
- *Would the individuals expect you to use their data in this way?*

Identifiable secondary care data is entered by hospital staff across England and Wales into a bespoke web-based audit tool provided by Crown Informatics Limited.
Health data is categorised as special category data and collected as part of the audits, aligned with the section 251 approval to collect such data.
For the NHFD, Crown Informatics securely transfer identifiable data (NHS number, DOB, Postcode, Name) to NHS England to link data and provide appropriate HES and Civil Registration data.
Linked data is returned to Crown Informatics, which combines the validated identifiers, NHS England and the NHFD data. This is then pseudonymised and securely transferred to University of Bristol for analysis.
Following the cleaning and analysis aggregated and anonymised data are also transferred from Bristol 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 Access Review Group (DARG). Data are released securely from Crown informatics, or if the applicant requires linked data, identifiable data is sent from Crown Informatics to NHS England with subsequent flow of a linked (de-identified) dataset from NHS England to the applicant organisation.

We have multiple ways of informing healthcare providers and patients of how the data is used and these are promoted to participated sites for further dissemination:
https://www.rcp.ac.uk/improving-care/national-clinical-audits/falls-and-fragility-fracture-audit-programme-fffap/fffap-data-processing-statements/

Stage 4: Necessity and proportionality assessment

*What is your **lawful basis** for processing under the UK GDPR and the UK Data Protection Act 2018?*

Legal basis: Section 251 across the three audits (England and Wales)
GDPR
o Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is justified through commissioning arrangements which link back to NHS England, Welsh Government and other national bodies with statutory responsibilities to improve quality of health care services.
o Article 9 (2) (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. This is justified as all projects aim to drive improvements in the quality and safety of care and to improve outcomes for patients.
DPA 2018 Schedule 1 condition for processing: Data Protection Act 2018 (legislation.gov.uk)
3. This condition is met if the processing—
(b) Is carried out by -
(i) by or under the responsibility of a health professional

*What additional **condition (including applicable legal basis under the common law duty of confidentiality)** are you relying on for processing special category data?*

Approval under section 251 of the NHS Act of 2006.

Transparency:

When you collect the data, will you be giving individuals the following information, in the form of a privacy notice/fair processing notice?:

a. *Identity of the data controller and contact details for the Data Protection Officer?*
b. *The purposes for which their data will be processed?*
c. *Length of time that the data will be retained?*
d. *The people or organisations their data will be shared with?*
e. *The lawful basis for processing their data?*
f. *Any international transfers of their personal data*
g. *When their personal data will be erased?*
h. *Their rights under GDPR?*

Please include a link to the privacy notice/fair processing statement which will be made available to individuals whose data is being processed.

https://www.rcp.ac.uk/improving-care/national-clinical-audits/falls-and-fragility-fracture-audit-programme-fffap/fffap-data-processing-statements/

Data minimisation:

a. *Is the personal data to be collected the minimum necessary to achieve your purpose(s)?*
b. *Will access to the data be restricted to those with a strict need to know?*
c. *How will access be controlled?*
d. *Is there any scope to anonymise or pseudonymise the data, and if not, why?*

For NHFD (and NAIF data prior to 2025 dataset): 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.
For NHFD, NAIF and FLS-DB:
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 and deprivation.
Postcode is retained 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 is used for social deprivation analysis to assess inequalities.

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.

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 (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN) fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre. Crown Informatics holds NCSC 'Cyber Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown Informatics and have login details to a secure webtool to access audit data.

Security:

a. *Will data be collected, transmitted and stored securely?*
b. *Is the level of security to be provided appropriate to the risks presented by the processing?*
c. *Will arrangements be put in place for the secure disposal and/or destruction of data when it is no longer required?*
d. *List the security measures used to protect the data or attach/provide a link*

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 at each hospital have access to the data, and only the individual units themselves can see the PIDs of their own patients (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN) fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre, certified to ISO 27001.
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.
Crown Informatics holds NCSC 'Cyber Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown Informatics and have login details to a secure webtool to access audit data.
University of Bristol – Bristol Medical School information security policy is listed below
http://www.bristol.ac.uk/infosec/policies/
http://www.bristol.ac.uk/secretary/data-protection/policy/

Data processors:

a. *Will a third party be used to process the data on behalf of your organisation?*
b. *What processing will the processor carry out?*
c. *Is there an agreement in place with the third party?*
d. *Does the agreement include all the provisions required under the GDPR?*

Working with the RCP, as their authorised data processor, Crown Informatics is commissioned and contractually bound to uphold strict information governance in respect of:

• Data Protection Act 2018 (RCP Registration: Z708553, Crown Informatics registration: Z3566445)
• EU General Data Protection Regulation (EU) 2016/679 (GDPR)
• NHS IG-Toolkit Statements of Compliance (Crown Informatics NHS ODS reference: 8J157, RCP reference 8J008)
• Data Sharing and Transfer Agreements duly authorised by the joint data controllers (HQIP, NHS England and Digital Health and Care Wales)
• All staff handling patient data are IG trained and bound by confidentiality agreements.

University of Bristol provide data analysis, at a pseudonymised level. University of Bristol is contractually bound to uphold the information governance in respect of:

- EU General Data Protection Regulation (EU) 2016/679 (GDPR)
- NHS IG-Toolkit Statements of Conformance/Compliance (ODS Code: EE133799-BRMS)

Pseudonymised patient level audit data is sent to University of Bristol for data cleaning and analysis.
University of Bristol
Following the cleaning and analysis of data, aggregated (i.e. analysed and non-identifiable) data will be transferred from University of Bristol to the RCP to provide commentary for, and then publication on, outcome-related audit programme outputs (e.g. national, trust and health board level reports).
Report writing aggregated data is sent to Royal College of Physicians to draft audit outputs (e.g. national reports). In addition, publicly available site (NHFD)/service level real-time run charts are made available via the Crown web-tool.
University of Bristol publishes research findings using the aggregated data. Small numbers are suppressed throughout.

Data sharing:

a. *Are decisions about how the data will be used being taken jointly with another organisation?*
b. *Is the data to be shared with that other organisation?*
c. *Is there an agreement with the other organisation covering respective roles & responsibilities including request and complaints handling?*

No.
HQIP and NHS England are the joint data controllers, any data release outside of that outlined in the data flows are to be sent via formal data access request forms and a data agreements in place ahead of release.

International transfers:

a. *Will data be transferred outside the **UK or EEA**?* b. *If so, will the transfer be to a country which has an adequacy decision recognised by the UK?* c. *If not, will appropriate safeguards be in place e.g., standard contractual clauses/data transfer agreements, etc?*
No

Stage 5: Risk assessment and mitigation

Outline any risks associated with the processing of the data.
Describe the likelihood of occurrence of the risk and the potential impact on individuals.
Include associated compliance and corporate risks as necessary.
Include any measures taken to reduce or eliminate the identified risks.
Assess risk after mitigation measures have been applied.

1. Impact on Individuals
(Will the processing lead to individuals suffering)

Risks of processing	**Likelihood/ Impact of harm** Low Medium High	**Overall risk** Low Medium High	**Measure taken to reduce or eliminate risk**	**Risk** Reduced Eliminated Accepted
Inability to exercise their privacy rights (e.g., right to access their personal data, request correction, request erasure, restrict processing, object to personal data being processed for marketing purposes or object to automated decision making and profiling)	Low/Medium	Low	Information shared in the fair processing statements on how to contact hospitals for personal data access. 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 patient's data is solely with the hospital/health and social care service who are entering the data. **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.	Reduced

Illegitimate access to information	Medium	Medium	Crown Informatics Ltd holds all identifiable information on behalf of FFFAP. The FFFAP team and Bristol 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 (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN) fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre. Crown Informatics holds NCSC 'Cyber Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown Informatics and have login details to a secure webtool to access audit data.	Reduced
Disappearance of data	Low/Medium	Low	Crown Informatics Ltd backups are encrypted at AES256, held in dual copies, and stored securely.	Reduced
Network failure (RCP)	Low/High	Medium	Data security at RCP. Data is regularly backed up on a server, and access to both servers comply with ISO27001 and Cyber Essentials plus certified. This will ensure that despite a network failure access can still be gained to key information.	Reduced
Sub-contractor network failure or cyber-attack	Low/Medium	Low	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 at each hospital have access to the data, and only the individual units themselves can see the PIDs of their own patients (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN)	Reduced

			fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre, certified to ISO 27001. Crown Informatics holds NCSC 'Cyber Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown Informatics and have login details to a secure webtool to access audit data. University of Bristol – Bristol Medical School information security policy is listed below http://www.bristol.ac.uk/infosec/policies/ http://www.bristol.ac.uk/secretary/data-protection/policy/	
Data breach: The audit programme has 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	Low/High	Medium	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 at each hospital have access to the data, and only the individual units themselves can see the PIDs of their own patients (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN) fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre, certified to ISO 27001. Crown Informatics holds NCSC 'Cyber Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown	Reduced

			Informatics and have login details to a secure webtool to access audit data. - Data security at RCP and ICL. Data is regularly backed up on a server, and access to both servers are certified to ISO 27001, the recognised standard for data security. University of Bristol – Bristol Medical School information security policy is listed below http://www.bristol.ac.uk/infosec/policies/ http://www.bristol.ac.uk/secretary/data-protection/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.	
Re-identification of pseudonymised data	Low/Medium	Low	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 at each hospital have access to the data, and only the individual units themselves can see the PIDs of their own patients (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN) fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre, certified to ISO 27001.	Reduced

			Crown Informatics holds NCSC 'Cyber Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown Informatics and have login details to a secure webtool to access audit data. - Data security at RCP and ICL. Data is regularly backed up on a server, and access to both servers are certified to ISO 27001, the recognised standard for data security. Only aggregate data is released in publications, as per the data flows. Small numbers are suppressed throughout.	
2. Source of risk to individuals *(A breach of security leading to individuals suffering)*				
Risks of processing	**Likelihood/ Impact of harm** Low Medium High	**Overall risk** Low Medium High	**Measure taken to reduce or eliminate risk**	**Risk** Reduced Eliminated Accepted
Loss, destruction, or alteration of personal data as a result of: • *Insecure electronic devices* • *Unencrypted memory sticks* • *Paper copies removed from secure work environment* • *IT system*	Low/High	Medium	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 at each hospital have access to the data, and only the individual units themselves can see the PIDs of their own patients (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN) fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre, certified to ISO 27001. Crown Informatics holds NCSC 'Cyber	Reduced

			Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown Informatics and have login details to a secure webtool to access audit data. - Data security at RCP and ICL. Data is regularly backed up on a server, and access to both servers are certified to ISO 27001, the recognised standard for data security.	
Inability to access personal data due to unavailable systems for processing, or inability of the organisation or a third-party provider to restore access to systems in a timely manner	Low/High	Medium	Data security at RCP. Data is regularly backed up on a server, and access to both servers comply with ISO27001 and Cyber Essentials plus certified. This will ensure that despite a network failure access can still be gained to key information. 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 at each hospital have access to the data, and only the individual units themselves can see the PIDs of their own patients (plus other duly authorised nominated users/administrators). Access to data is via secure client software, operating over secure internet (or VPN) fire walled networks plus additional secondary application layer security. Data is stored at a professionally operated, secure data centre, certified to ISO 27001. Crown Informatics holds NCSC 'Cyber Essential Plus' certification and is compliant with the NHS 'Data Protection and Security Toolkit' requirements. All users that have access to identifiable data have to be registered with Crown Informatics and have login details to a secure webtool to access audit data.	Reduced

			University of Bristol – Bristol Medical School information security policy is listed below http://www.bristol.ac.uk/infosec/policies/ http://www.bristol.ac.uk/secretary/data-protection/policy/	
3. Compliance / corporate risk *(Is the processing likely to result in)*				
Risks of processing	**Likelihood/ Impact of harm** Low Medium High	**Overall risk** Low Medium High	**Measure taken to reduce or eliminate risk**	**Risk** Reduced Eliminated Accepted
The organisation's non-compliance with Data Protection legislation and IG requirements	Low/High	Medium	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 processes and the dates that they are due. Reminders are placed in calendars and in project plans to ensure all necessary team members are aware of the requirement to update these essential documents and approvals.	Reduced
National Data Opt-out risk	Low	Low	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 patient's data is solely with the hospital/health and social care service who are entering the data. This does not apply in Wales. There are regular discussions with HQIP regarding compliance and to ensure a	Reduced

			consistent approach across the programme. At present the NDOO only applies to FLS-DB as NHFD and NAIF received exemption. FLS-DB have produced supporting documents, videos and webinars to help services comply with the process.	
Financial or reputational risks to organisation or HQIP as the data controller	Low/High	Medium	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. The audit programme will ensure that the audits are covered under Section 251 of the Health and Social Care Act. There is a risk that S251 approvals are not submitted in time for annual renewals. - 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 Univeristy of Bristol Data is regularly backed up on a server, and access to both servers are certified to ISA 7001, the recognised standard for data security. - All members of the audit team have data protection training on an annual basis. - All members of the audit team have been trained in cyber security. - FFFAP team will stay up to date with data regulations, including national data opt out and GDPR to ensure compliance.	Reduced

			- As a secondary measure to national data opt out at a local level, Crown will also carry out screening of data prior to data release. To reduce the risk of section 251 delays/not being obtained in time, all managers will be aware of the renewal date. The IG lead for the FFFAP team will work with the project managers to ensure consistency and high standards of the s251 applications, both renewal and amendments, and ensure they are submitted on time so as to not impact on the ability of the projects to collect data. To reduce the risk of releasing data to third parties and potential data breach, the following steps have been taken to mitigate this risk: - The scientific and publications committee will comprehensively review all applications prior to them being sent to HQIP. - The HQIP DARF process will be followed comprehensively. - No data will be transferred that has not gone through the above two processes. - Small number suppression will be applied to data outputs and transparency data to reduce reidentification.	