Protect

Fraud Information Reporting System Toolkit (FIRST)

Privacy Impact Assessment

Version 2.0

This document contains information in relation to the method and scope of fraud investigations within the NHS, in particular considering elements in relation to individuals. As such it is deemed OFFICAL.

Any information viewed/obtained within this document should therefore be treated in the appropriate manner as detailed in the terms and conditions of use for this site and as advised by the Government Security Classifications (2014).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL and therefore there is no requirement to explicitly mark routine OFFICIAL information. However, any subset of OFFICIAL information which could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases, assets should be conspicuously marked: OFFICIAL–SENSITIVE'

Document Information	
Document Title	FIRST Privacy Impact Assessment
Author	Information and Records Management Officer
Date	January 2017

Document Control					
PM	**Ref**	**Owner**	**Version No**	**Issue Date**	**Amendments**
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V0.1	02/02/2017	All
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V0.2	15/02/2017	General comments and corrections
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V0.3	17/02/2017	Requested amendments from review
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V1.0	27/02/2017	Finalised draft
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V1.1	20/04/2017	Updated draft
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V1.2	25/04/2017	Final amendments following comments
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V1.3	28/07/2017	Further amendments following review by DPO
Information and Records Management Officer	PIA/FIRST/ 2017	DPO	V2.0	27/03/2019	Version no updated prior to publication

Preface

Fraud Information Reporting System Toolkit (FIRST)

Reference:	PIA/FIRST/2017
Date:	January 2017
Author:	Information and Records Management Officer
Owner:	National Operations Manager
Version:	2.0
Supersedes:	1.3

Contents List

Links & Dependencies

Document	Title	Reference	Date	POC
Government Security Classifications	Government Security Classifications	All	April 2014	Cabinet Office
EU GDPR	**EU General Data Protection Regulation**	All	May 2018	GDPR
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	Infosec Standard 2	Issue 3.2	January 2010	CESG
DPA	Data Protection Act	All	1998	HMG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG
HRA	Human Rights Act	All	1998	HMG
FOI	Freedom of Information Act	All	2000	HMG

Table 1 – Links and Dependencies

Section 1: Privacy Impact Assessment Requirement

Introduction

1. Although the Information Commissioner's Office ("ICO") has not decreed that there is a legal obligation to undertake a Privacy Impact Assessment ("PIA") on systems holding personal or private data, all HMG departments are being mandated to conduct an assessment. NHS Protect has agreed that all systems holding data on more than 250 people will require a PIA.

2. The PIA is a process that enables organisations to anticipate, identify and address the potential privacy impacts of new initiatives or systems. The identified risks to an individual's privacy can be managed through consultation with key stakeholders and where applicable systems can be designed to avoid unnecessary privacy intrusion.

3. Within NHS Protect all systems that process or store personal data on more than 250 people require a PIA to be conducted and documented as part of the accreditation evidence. This PIA is related to, and makes reference to, the NHS Protect FIRST specific Risk Management & Accreditation Document Set ("RMADS"), which is the name given to a series of documents that outline the threats, risks and security countermeasures in detail for FIRST, as well as a series of models that calculate threat actors, domain layout and the general makeup of the FIRST system. The RMADS also contains the initial PIA completed on creation of this system, which this document supersedes. The RMADS was developed in accordance with the requirements of NHS Protect and CESG HMG Infosec Standards 1 and 2 and contain the following documents.

FIRST General Description

4. The NHS Protect Fraud Information Reporting System Toolkit ("FIRST") is an information gathering, intelligence disseminating case management tool designed and provided specifically for all Area Fraud Specialists ("AFS") and Local Counter Fraud Specialists ("LCFS") by NHS Protect.

FIRST helps AFSs/LSCFs to manage referrals, intelligence, fraud enquires, case preparation and a range of other investigative tasks and includes useful editing tools that help to keep information and cases up to date.

FIRST is owned and operated by NHS Protect and its use is mandatory for everyone engaged in the investigation of fraud within the NHS.

5. FIRST is required to comply with relevant HMG legislation including where applicable the Data Protection Act 1998, Human Rights Act 1998 and Freedom of Information Act 2000. To ensure that FIRST meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a PIA which is broken down into the following stages:

a. PIA Screening. (This is a condensed screening process using the NHS Protect adapted Pre Privacy Impact Assessment Questionnaire. The output will determine if a PIA is required and indicate how much effort is required depending on the type, quantity and sensitivity of the personal information involved).

b. PIA Assessment and Report;

c. Compliance Checks;

d. Summary and Conclusions.

Ownership

6. The following tables describes the FIRST roles and responsibilities:

Role	Responsibility
Information Asset Owner (IAO)	National Operations Manager
Senior Responsible Officer (SRO)	Head of Intelligence and Crime Prevention
Application Owner	National Operations Manager
Data Protection Officer	Information Governance & Risk Management Lead

Section 2: PIA Screening

The PIA Screening Process

1. The initial PIA screening process determines if a PIA is required to be conducted. The decision is based on the quantity and sensitivity of the personal data being processed and any privacy impacts. The categorisation of sensitive personal data is described in Annex A.

2. The screening process has used the NHS Protect Pre Privacy Assessment Questionnaire to determine whether a PIA is required. The intention of the questionnaire is not to provide over elaborate answers but to demonstrate that all aspects of the project have been considered regarding personal data. Once completed, the IAO and DPO are required to assess the responses to determine if a PIA needs to be conducted. The responses provided in the Pre PIA Questionnaire and DPO/IAO decision are to be made available to the Accreditor.

3. **The ICO PIA template notes that organisations can choose to adapt the process and the PIA template to produce something that allows them to conduct effective PIAs integrated with the project management processes and fits more closely with the types of project likely to be assessed. Therefore, this is a NHS Protect specific questionnaire and slightly differs from the ICO screening questionnaire, whilst covering the same issues and content.**

Ser	Question	Response
1	System/Application/Project Name	Fraud Information Reporting System Toolkit (FIRST)
2	What is the main function of the System/Application/Project?	An online case management tool designed to assist everyone engaged in the investigation of fraud within the NHS. The tool gathers information and disseminates intelligence, assisting those investigating fraud with the following: • Conducting investigations • Managing referrals • Intelligence • Fraud enquires • Case preparation • Applying appropriate sanctions and financial recovery.

3	Briefly, what are the personal data elements used by the System/Application/Project? See Annex A for guidance,	Information that can be used to identify a living person Information which, if subject to unauthorised release, could cause harm or distress to an individual Sensitive personal data relating to an identifiable living individual
4	What [1]personal data is collected? (See Annex A for definitions)	**The following personal data is captured by FIRST, please note this is not the full dataset, which is identified fully in Annex B** Name (also for source /witness/contacts) Date of birth (also for witness/contacts) Address (also for source / witness/contacts) Contact Details (also source & witness/contacts) Nationality NI Number Passport Number Ethnic Code NHS Number Driving Licence Number Payroll Number Professional Body Registration Number Other Identifier(could be any other ID) NHS Employment Details(also for witness) NHS Dept. where treatment delivered Details of links to NHS Any Other Occupation/Employment Description (inc height, hair - style, length and colour, facial hair, eye colour, body type, distinguishing features / marks and scars. Financial Details inc: name, address and phone number, sort code and account number. Vehicle Details inc: Make model, colour, age and licence registration plate. Details of credit history and other personal checks.

[1] Note the DEPT Chief Information Officers Department has confirmed that 'Business card' information should not be classed as personal information. Business Card Information includes: Name, Post/Role, Work Address and Contact details.

5	From who is the personal data collected?	Fraud information and evidence is gathered by NHS Protect from a variety of sources, information can be referred from the following organisations: NHS Health Bodies, NHS Foundation Trusts, Private Providers of NHS healthcare, NHS Commissioning Organisations. Department of Work and Pensions, Financial Institutions, Local Authorities, Media, NHS Source, Police Regulatory Bodies and Professional Bodies inc General Medical Council. (GMC) General Optical Council (GOC), General Pharmaceutical Council (GPhC) Medicines and Healthcare Regulatory Agency (MHRA) Third party checking sources i.e credit reference agencies. Additionally, member of the public are able to report concerns about fraud and corruption in the NHS by telephone to NHS Protect via the Fraud and Corruption Reporting Line (FCRL) and via an online (FCROL)
6	Why is the personal data being collected?	It is collected for the purpose of investigation and to identify the subject. Additionally, background information is necessary as it assists in determining all of the circumstances. The entirety of the data is required for the following purposes: • Supporting fraud investigations by extracting and analysing data for individual cases • Developing processes to identify the scale of fraud • Applying knowledge from previous cases to identify further fraudulent activity • Identify irregular patterns which are indicative of fraud
7	How is the personal data collected?	Data is input manually via a secure web portal using https secure 256 bit encryption.

8	Describe all the uses for the personal data (including for test purposes).	Section 6, in explaining why this data is captured provides some insight into how it is used in the sense of objectives and functions. However for more specific descriptions to the actual steps necessary to achieve these purposes, personal data is used alongside the rest of the dataset in the following ways: • To identify the Subject of an investigation in relation to fraud bribery and corruption within the NHS and to assist in the recovery of funds obtained dishonestly. Through analysis of the relevant datasets, identifying high risk areas and how Information Analytics could use this data to identify fraudulent behaviour. • Establishing normative behaviour within the data, as a means to identify outliers against the rules identified • Engaging with in-house Fraud Specialists and Fraud Investigators, to gain overview of irregular areas and their viability for further action, including how they can be gathered, collected and produced to support closer examination. • Agree criteria for output format to the above internal stakeholders in light of producing data for the purposes of supporting investigations and supporting criminal investigations • Setup reporting timeframes and format for continuous improvement of efficient and effective data processing • Evaluate known outcomes and priorities and action next steps for continuous dissemination and additional analysis There is no use of personal data for testing
9	Does the system analyse the personal data to assist Users in identifying previously unknown areas of note, concern or pattern?	Yes, the system is designed to analyse at a national and local level to provide trends in relation to crime within the NHS and to assist with Investigations.
10	Is the personal data shared within internal organisations?	Yes

11	For each organisation, what personal data is shared and for what purpose?	All of the personal data identified in section 4 could potentially be shared internally with NHS Protect. The purpose as described fully in section 8 is to identify the Subject of an investigation in relation to fraud bribery and corruption within the NHS and to assist in the recovery of funds that were dishonestly obtained.
12	Is personal data shared with external organisations? (If No go to Q15)	Potentially
13	Is personal data shared with external organisations that are not within the [2]European Economic Area?	No
14	For each external organisation, what personal data is shared and for what purpose?	Information from FIRST may be shared with external organisations depending on the severity of the investigation and the course it takes. Data may be shared with the LCFS at the trust if the investigation results in a Disciplinary. Data may be shared with the CPS/ Police or other Professional body if the investigation results in a successful prosecution through the courts and a Civil or Criminal sanction obtained.
15	How is the personal data transmitted or disclosed to internal and external organisations?	Via a Secure web portal using 256 bit encryption.
16	How is the shared personal data secured by the recipient?	There is no downloading of investigations reported to FIRST, only direct inputting of data. Because FIRST is a permission-based application, users can only access records for which they have responsibility. All other personal information submitted by other users is anonymised.

[2] Norway, Iceland and Lichtenstein together with other European Union Nations and Switzerland make up the European Economic Area.

17	Which User group(s) will have access to the system?	Local Counter Fraud Specialists (LCFS) (access only to prepared reports and their own submitted data) NHS Protect Anti Fraud Specialists (AFS) (access only to prepared reports and their own submitted data) Information Analytics NHS Protect Staff Systems Administrators Non Information Analytics NHS Protect Staff (access only to prepared reports, not incident data itself)
18	Will contractors/service providers to NHS Protect have access to the system?	No
19	Does the system use "roles" to assign privileges to users of the system?	Yes
20	How are the actual assignments of roles and rules verified according to established security and auditing procedures?	Non NHS Protect Staff: Access to FIRST can only be gained by NHS accredited AFSs, LCFSs or other authorised users who hold a current nomination and who, in the case of LCFSs, are currently employed by an NHS body directly, or through a third party organisation, to perform the LCFS role on its behalf. LCFSs are nominated by Health Bodies and accredited by NHS Protect. NHS Protect Staff System administrators have full access to all data tables (including encrypted tables containing personal data) Information Analytics NHS Protect staff have access to the non-encrypted data tables and prepared reports Non Information Analytics NHS Protect staff only have access to prepared reports
21	What is the current accreditation of the system?	Official (Sensitive)

Table 2 - PIA Screening Questionnaire

4. Having completed the questions in the table above it should be possible to confirm what type of personal data is being processed by the system/application and whether a PIA is required and the type and level of detail required. Essentially if any of the responses to questions 1-3 is yes then a PIA is required. The following questions are mandatory and must be completed:

Ser	Question	Response
1	Will personal data be processed, stored or transmitted by the system/application? (If No go to Q4)	Yes
2	Will the project process, store or transmit more than 250 Personal Data records (If No go to Q3)	Yes
3	Will [3]sensitive personal data be processed, stored or transmitted by the system/application?	Yes
4	Is a PIA required for the system / application? (If No go to signature block)	Yes
5	What level of scale of PIA is required? (Guidance should be sought from the DPO, IAO and Accreditor)	Full

Screening Process Conclusions

5. The screening process, completed in January 2017, identified the following PIA requirements of using the FIRST application.

a. A Privacy Impact Assessment (PIA) is required.

b. The PIA should after consultation with the DPO, IAO and Accreditor be completed in accordance with the NHS Protect PIA template which is based on the full scale assessment. The requirements from which this template was derived are described on the ICO website at http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/26-report.html

c. A number of legal requirements apply to FIRST and are referenced and included in the RMADS, User System Operating Procedures ("SyOPs") and all operating procedures and therefore must be included within this PIA in a manner that is consistently applied. The relevant applicable legislation is:

i. Data Protection Act 1998

ii. Human Rights Act 1998

iii. Freedom of Information Act 2000

[3] Sensitive personal data is personal data that consists of racial or ethnic origin, political opinions, religious beliefs etc – full details of sensitive personal data is available in the Data Protection Act 1998, see Annex A.

6. The conclusion reached following the review of this screening is that,

    a. There is great benefit to having a documented list of the considerations related to the processing of personal data within the FIRST system, including the purposes for which it is gathered and outputs it produces.

    b. This benefit is increased further when it is considered that some elements of the data capture are potentially contentious (i.e. personal data in relation to subjects), and that documented evidence of the considerations surrounding them and justifications for use is additionally of benefit and can provide assurance.

Section 3: Privacy Impact Assessment & Process

Introduction

1. A PIA is defined as a process whereby the potential privacy impacts of a project are identified and examined from the perspectives of all stakeholders in order to find ways to minimise or avoid them. Ideally, PIAs should be undertaken at the beginning of the project's life cycle so that any necessary measures and design features are built in; this minimises the risk to the project both in terms of ensuring legal compliance and addition of costly retrospective security controls.

2. The PIA screening process concluded in 2017 that although not undertaken at the beginning of the project, a requirement for a Full PIA was required based on the type and quantity of personal data involved.

PIA Phases

3. The ICO PIA Handbook suggests 5 phases to a PIA:

a. Preliminary Phase – This phase establishes the scope of the PIA, how it is going to be approached and identifies tasks, resources and constraints.

b. Preparatory Phase – This phase organises and makes arrangements for the next phase of the process; the Consultation and Stakeholder analysis;

c. Consultation and Analysis Phase – This phase focuses on consultation with the system stakeholders (including clients/customer where applicable), risk analysis with respect to privacy, recognition of privacy issues and identification of potential solutions;

d. Documentation Phase – This phase documents the results of the Consultation and Analysis Phase to include a summary of issues and proposed actions, where required;

e. Review and Audit Phase – The review and audit process is maintained until the system or application is decommissioned and disposed of. Reviews and audits should be conducted annually or at times of significant change to ensure that there is no change of impact or risk with respect to privacy.

Approach

4. FIRST became operational amongst NHS Protect staff in August 2009 with delivery to the national Local Counter Fraud Specialist network following in December 2009. This is the first Privacy Impact Assessment on the system and as such, all content, considerations and assessments are based on existing fraud arrangements in place within NHS Protect for similar datasets, based on effective counter fraud work completed in the past.

5. FIRST is a system in widespread use across the NHS and has undergone some development since its introduction in 2009. This PIA is developed by the Information Analytics Lead, in consultation with NHSProtect staff from a number or teams.

Section 4: PIA Report

Executive Summary

1. The FIRST System records personal data on the source, the subject and the witness/contact of an NHS Investigation. This information includes the following:

    a. **For the source:**
        - Name, address and contact details of the source of the information.

    b. **For the subject:**
        - Name, address and contact details.
        - Date of birth,
        - Nationality and Passport Number
        - NI number
        - NHS Number
        - Racial or ethnic origin
        - Driving licence number
        - Payroll number
        - Details of professional body including registration number
        - NHS employment details
        - NHS department where any treatment is being received
        - Details of any other occupation/employment
        - Full description including height, hair style, length and colour, whether any facial hair, eye colour, body type, and if there are any distinguishing features marks or scars.
        - Bank Details including name, address and phone number, sort code and account number.
        - Vehicle Details including make, model, colour, age and licence registration plate.
        - Details of any commission or alleged commission of offences, proceedings and outcomes relating to an actual or alleged offence.
        - Details of credit history and other personal checks

    c. For the Witness:
        - Name, address, date of birth, contact details and employment information.

2. The impact level of the FIRST information was assessed at OFFICIAL and OFFICIAL SENSITIVE. However the OFFICIAL SENSITIVE classification only applies to internal NHSP staff and DH Anti Fraud unit.

3. The following measures briefly describe what controls have been implemented to protect FIRST and the personal data recorded in the application:

    a. All personal information listed above is encrypted upon receipt into the FIRST system. The data is decrypted when the server is started up and the decryption key entered by the Data Base Administrator.

    b. All off site back-ups are secure as they can only be opened via the encryption key.

    c. An additional level of data security is the Virtual Private Database (VPD) which automatically restricts access to cases once they are classified as confidential. A case can start off as restricted and be accessed by the LCFS and assigned NHSProtect staff. However if the classification of the case is upgraded to confidential then the LCFS would no longer be able to access.

d. All LCFS users are granted access to the system by the NHS Protect Service Desk, following receipt of a completed nomination form authorised by the responsible Director of Finance (DOF) at the NHS body.

e. LCFSs only have access to their own cases of which they have created or been assigned.

f. There are no direct interfaces / interconnections with other systems or applications, however specific data may be exported from FIRST and subsequently imported to other programmes as part of an automatic process.

g. There is functionality within the application to export data to the CPS as prosecution files.

h. The FIRST Data Custodian must comply with the data protection requirements described in the FIRST User Manual. Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSP register and the NHS Protect DPO is aware of its existence.

i. FIRST login passwords expire every 30 days, additionally a report is available to review activity on the system of when users have last logged in.

4. It is assessed that there are no residual privacy risks to the personal data used by the FIRST application. Risks to confidentiality are listed in the Risk table below and documented in the FIRST RMADS.

Introduction

5. FIRST is an application designed and developed by NHS Protect. Any information received in relation to the suspicion of fraud bribery or corruption within the NHS is entered in to the system as a piece of information. A case will be created from the information only when any suspicion is confirmed.

Section 1: Data Collection and Maintenance

6. Personal data collected by the application includes details of the subjects of fraud investigations

For the source: name address and contact details.

For the subject: Name, address, date of birth, contact details, nationality, NI number, passport number, racial or ethnic origin, NHS number, driving licence number, payroll number, details of professional body including registration number, NHS employment details or any links to NHS including department where treatment is being received, details of any other occupation/employment, full description including height, hair style, length and colour, whether any facial hair, eye colour, body type, and if there are any distinguishing features marks or scars. Bank Details including name, address and phone number, sort code and account number, Vehicle Details including make, model, colour, age and licence registration plate. Details of any commission or alleged commission of offences, Proceedings and outcomes relating to an actual or alleged offence, Details of credit history and other personal checks

For the witness: name, address, date of birth, contact details and employment information.

Additionally, there may be circumstances where the alleged perpetrator is a non NHS-Subject in which case the Company name, SIC Code, Registration Number, Incorporation Date, VAT Number, Trading Address and Registered Address will also be included.

7. This PIA must be reviewed if any changes are made to the personal information if used by the FIRST application or any other changes are made that affect the privacy of an individual.

8. The privacy risks to the individual subject are subtly different to the confidentiality risks that have been documented in the FIRST RMADS documentation. The privacy risks and associated mitigations are described in Table 4, which reflects similar risks identified in the FIRST Project Risk Register. The IAO is responsible for mitigating the risk and their responsibilities are defined in the FIRST SyOPs.

Risk Description	Mitigation
1. There is a risk that the personal data is used for other purposes than for what it was originally intended for.	All personal data received by NHS Protect is encrypted upon receipt. Access to this data is only possible via the Database Administrators, via a login and password Users are only given sufficient rights to systems to enable them to perform their specific job function. User rights will be kept to the minimum required to do their job effectively and efficiently. Access rights are reviewed on a monthly basis.
2. There is a risk that excessive personal data is collected on an individual.	This PIA exists to ensure that there is due consideration as to the extent of the data used. There is no adequate way to assess the extent of the data that is relatable to fraud investigations prior to receipt and analysis. Data not related to fraudulent activity can be used to identify normative behaviour which can then strengthen the analysis. The content of the data has been examined to ensure it is only what is essential to perform this analysis and draw these findings.
3. There is a risk that personal data is retained for longer than necessary.	FIRST is subject to NHSBSA NHS BSA Data Handling and Storage Policy and is audited annually to ensure that personal data is not retained longer than necessary.
4. There is a risk that the personal data is no longer relevant.	Relevance of personal data is one of the aspects considered during the review. Given that the personal data gathered is always specific to an investigation of fraud, bribery or corruption, the data will always be relevant as individually it provides a case study of the investigation and in bulk it can be used to profile perpetrators and produce trends in relation to Fraud within the NHS.
5. There is a risk that the personal data is not accurate or up to date.	FIRST data is provided by various sources and updated as the investigation progresses. As such, the responsibility for accuracy lies with the investigating officer. However there is no process possible to routinely ensure the information is accurate and up to date; the data is updated when inaccuracies are discovered. As there is no means to audit or review for accuracy – information is assumed accurate as provided (but caution is applied for use as a result)

Risk Description	Mitigation
6. There is a risk that the confidentiality of the personal data is not adequately protected.	All risks in relation to security and other protective measures are identified in the FIRST RMADS documentation all risks relating to confidentiality have been mitigated as far as possible.
7. There is a risk that personal data is passed to external organisations.	No personally identifiable information will be passed on to external organisation other than as outlined in section 14 above as it contravenes data protection. However for statistical purposes only, non-identifiable information will be shared in the following contexts: 1. Statistical data (i.e. tables and graphs) produced in relation to the personal data of alleged suspects, without any details of individuals or the means to link it to actual persons or specific incidents. 2. Outcomes of convictions without any details of individuals or the means to link it to actual persons or specific incidents.
8. There is a risk that personal data is hosted or exported outside of the EU.	FIRST will only be hosted in the UK and no data will be exported outside the UK

Table 4 – Privacy Risks

Section 2: Uses of the Application and the Data

9. FIRST holds details of investigations relating to fraud, bribery and corruption within the NHS.

10. The information is collected for the identification and analysis of suspects involved in acts of fraud bribery and corruption within the NHS.

11. The measures that have been implemented to protect the Personal Data are:

a. The number of FIRST Users is limited to Accredited Local Counter Fraud Specialists (LCFSs) along with a select number of internal staff from NHS Protect. There is currently an expectation of no more than 1000 Users of the application.

b. Access to FIRST can only be gained by NHS accredited AFSs, LCFSs or other authorised users who hold a current nomination and who, in the case of LCFSs, are currently employed by an NHS body directly, or through a third party organisation, to perform the LCFS role on its behalf.

c. All Users account creation, passwords and access have to be authorised by the NHS Protect Service Desk.

d. FIRST passwords expire every 30 days and users are prompted to reset by entering the old password and selecting a new one in the required format.

e. There are no direct interfaces / interconnections with other systems or applications, however specific data may be exported from FIRST and subsequently imported to other programmes as part of an automatic process.

f. There is no functionality within the application to export data to the file system or removable media i.e: CPS file transfer and MG Forms

g. The FIRST IAO must comply with the data protection requirements described in the FIRST Risk Management and Accreditation Document Set (RMADS) and FIRST Manual. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

12. Data will be retained only as long as necessary, up to a maximum period in accordance with the Data Protection Act 1998. The maximum period depends on whether fraudulent behaviour is detected – if fraud is found then the retention period is 7 Years, if fraud not found then its 3 years. The data will be stored in digital format and will be erased, using a CESG approved product (Blanco), from the relevant storage server when no longer required. The IAO is required to review the retention period as described in the FIRST SyOPs and if there is a requirement to change the retention period the change must be submitted to the Application Change Board.

13. The current retention schedule as detailed above has been approved by the Data Protection Officer.

Section 4: Internal Sharing and Disclosure of Data

14. Within NHS Protect, non-personal FIRST data is accessible to authorised users of FIRST and the SAS system, It is important to note that none of these users will have access to unencrypted personal data without written approval from the DO (with the exception of the Database Administrator)

Section 5: External Sharing and Disclosure of Data

15. No personally identifiable information will be shared with external organisations as it would contravene data protection. However for statistical purposes only, non-identifiable information will be shared in the following contexts.

a. Statistical data (i.e. tables and graphs) produced in relation to the personal data of alleged suspects, without any details of individuals or the means to link it to actual persons

b. Outcomes of convictions without any details of individuals or the means to link it to the actual persons.

Section 6: Notice/Signage

16. It would be inappropriate for NHS Protect to advise individuals of their data being processed, as the purpose for doing so is to uncover fraudulent behaviour and therefore notification may result in the behaviours changing/becoming more complex and therefore harder to detect.

17. NHS Protect hosts a subsection within the NHS Protect website entitled “How we handle data” ,within which this link is a document entitled “Q&A of data management ”. This broadly covers all elements of the NHS Protect usage of data, in a nonspecific manner.

18. The use of signage or other notifications to notify the public of the gathering and use of personal is not relevant to this dataset or the counter fraud project behind it, and therefore outside the scope of this PIA.

Section 7: Rights of Individuals to Access, Redress and Correct Data

19. Individuals have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHS Protect, We are required to provide the individual who has made the request with details of the personal data recorded about them, except where the usual exemptions may apply.

20. It is unlikely that many access requests will be received, as information about ongoing fraud investigations are themselves confidential until such point they are either substantiated – as such individuals would not know their data is being processed and any requests for information about individuals would only be proactive requests from those who may believe this is so.

21. Finally, in some cases the original records for each incident lie with the originating organisation, who would have greater levels of detail than is captured by FIRST in their local records and (as well as being the obvious choice for approaching for this data) would be the more appropriate point of contact.

22. In the unlikely event that that information in relation to the subject is identified as being incorrect the FIRST administrators may be asked to correct the record.

23. All NHS employees and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

24. The security and technical access architecture of the FIRST application is described in the FIRST RMADS. The application and the hosting infrastructure was assessed at Official and Official Sensitive. However the Official Sensitive classification only applies to internal NHSP staff and DH Anti Fraud unit. The application continues to be subject to CESG approved IT Security Health Checks

25. There is expected to be no more than approximately 1000 Users of the application which include: Nominated Accredited LCFS Users, NHSProtect Users and FIRST Application Administrators. LCFS and NHSP staffs have “read”, “create” and “modify” access while Application Administrators have “create” and can also manage application content. The Application Administrators also authorise new accounts. As the total number of User accounts is less than 1000, they are manually managed by the Administrators. The detailed procedures are described in the System Operating Procedure’s (SyOPs) section of the FIRST RMADS documentations.

26. The technical controls to protect the application and the FIRST information include:

a. Anti-virus protection;

b. Role based access controls;

c. Password complexity;

d. Patching Policy;

e. Media Management;

f. Encryption

g. Logging, audit and monitoring controls.

Section 9: Technology

27. FIRST is a web application hosted on the NHSP hosting infrastructure located in the NHSP data centre. It was developed ‘in house’ using the Java development framework.

Conclusion

28. There are no residual privacy risks to the personal data recorded in FIRST. The controls described in this PIA and RMADS documentation describe in detail how the data is protected and managed in accordance with the DPA98. The DPO is responsible for ensuring that the controls are implemented through the lifecycle of the system.

Section 5: Compliance Checks

DPA 98 Compliance Check

1. The DPO must ensure that FIRST, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

   a. The Data Protection Act in general;

   b. The Data Protection Principles;

   c. The interpretations of the Principles.

2. **This is not a recommendation but a requirement of law.**

3. The roles and responsibilities for the protection of personal data are described in the NHSP security policy.

4. The application process sensitive personal data so a Data Protection Compliance Check Sheet has been completed describing how the requirements of DPA98 have been complied with, see Annex C.

The Privacy and Electronic Communications Regulations

5. The Privacy and Electronic Communications Regulations are not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

6. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

7. As public authority we are compliant with the provisions of the Freedom of Information Act, in publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, there would be no personal information disclosed under the Freedom of Information Act as this would breach the data protection principles.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the Data Protection Act 1998 (DPA98).

Particular care must be taken with data in Category B and with any large data set (i.e. consisting of more than 250 records). Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints in DPA98 on the processing of data in Category C.

Annex B – FIRST Personal Data

1. The table below lists and describes all the personal data processed and stored in FIRST. It also includes a justification of the requirement for its use.

Ser	Personal Data	Justification
1	Name of Subject	Required to identify the subject of the investigation.
2	Date of Birth of Subject	Required to identify the subject of the investigation.
3	Address of Subject	Required to identify the subject of the investigation.
4	Contact details of Subject	Required for the purpose of the investigation.
5	Nationality of the Subject	To assist in the identification of the subject
6	NI Number of Subject	To assist in the identification of the subject and to establish their employment history.
7	Passport Number	To assist in the identification of the subject.
8	Ethnic Code	To assist in the identification of the subject.
9	NHS Number	Required for the purpose of the investigation
10	Driving Licence Number	Required for the purpose of the investigation
11	Payroll Number	Required for the purpose of the investigation
12	Professional Body / Registration Number	Required for the purpose of the investigation
13	NHS Employment Details	Required for the purpose of the investigation
14	Department where NHS Treatment received	Required for the purpose of the investigation

15	Personal Description: height, hair style, hair colour, facial hair, hair length, hair description, eye colour, body type. Distinguishing features / marks and scars.	Required for the purpose of the investigation
16	Bank Details	Required for the purpose of the investigation and in particular financial investigations.
17	Vehicle Details inc: make, model, colour, age, licence plate.	Required for the purpose of the investigation
18	Commission or alleged commission of offences	Required for the purpose of the investigation
19	Proceedings and outcomes relating to offences	Required for the purpose of the investigation
20	Details of credit history and other personal checks	To assist with the investigation
21	Name and address of source	To assist with the investigation
22	Contact details of source.	To assist with the investigation
23	Source type	To determine from what source the information was received.
24	Name and Address of Witness	To assist with the investigation
25	Date of Birth of Witness	To assist with the investigation
26	Contact details of witness	To assist with the investigation
27	Employment information of witness	To assist with the investigation

Annex C – Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHS Protect
Branch / Division	NHS Protect
Project	Fraud Information Reporting System Toolkit (FIRST)

2. Contact position and/or name, telephone number and e-mail address.
(This should be the name of the individual most qualified to respond to questions regarding the PIA)

Name, Title	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, NHS Protect
Phone Number	0191 2046311
E-Mail	Trevor.Duplessis@nhsprotect.gsi.gov.uk

3. Description of the programme / system / technology / legislation (initiative) being assessed.
(Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

The Fraud Information Reporting System Toolkit (FIRST) is an application that is designed to gather information and disseminate intelligence, to assist in investigations in relation to fraud bribery and corruption within the NHS.

FIRST became operational amongst NHS Protect staff in August 2009 with delivery to the national Local Counter Fraud Specialist network following in December 2009. This is the first Privacy Impact Assessment on the system and as such, all content, considerations and assessments are based on existing fraud arrangements in place within NHS Protect for similar datasets, based on effective counter fraud work completed in the past.

2. First is a system in widespread use across the NHS and has undergone some development since its introduction in 2009. This PIA is developed by the Information Analytics Lead, in consultation with NHSProtect staff from a number or teams.

4. Purpose / objectives of the initiative (if statutory, provide citation).

NHS Protect leads on a wide range of work to protect NHS staff and resources from crime. In particular, it has national responsibility for tackling fraud, as this has been identified a key activity that would otherwise undermine the effectiveness of the health service and its ability to meet the needs of patients and professionals.

To achieve this, NHS Protect collects data appropriate for preventing and detecting fraud within the NHS, remaining mindful that, where this includes personal data, the personal data is adequate, relevant and not excessive for the purposes for which it is processed.

In relation to the NHS BSA remit, Part 2, Section 12 of the NHS Business Services Authority Directions 2013 NHS Business Services Authority Directions4 2013 notes that the Authority must exercise (through NHS Protect) the functions in relation to counter fraud and security management specific in Schedule 1, which concerns itself with the functions of the authority in relation to counter fraud and security management.

Specifically, Section 9 of Schedule 1 notes the following function: "(to) obtain, monitor, collate and analyse such data as NHS Protect considers appropriate for the purposes of identifying trends and anomalies which may be indicative of fraud, corruption or other unlawful activities against or affecting the health service."

FIRST acts as an electronic tool which allows AFSs/LSCFs to manage referrals, intelligence, fraud enquires, case preparation and a range of other investigative tasks and includes useful editing tools that help to keep information and cases up to date.

Reporting on FIRST is enshrined in the following requirements:

- The NHS Standard Contract for providers, specifically clause 4.1 and 4.2 in relation to 'Hold to Account' states the following:
- 4.1: The organisation ensures that FIRST is used to record all reports of suspected fraud, bribery and corruption, to inform national intelligence. FIRST is also used to record all system weaknesses identified as a result of investigations and/or proactive prevention and detection exercises.
- 4.2 The organisation uses FIRST to support and progress the investigation of fraud, bribery and corruption allegations, in line with NHS Protect guidance.
- Section 5.2 of the NHS Anti Fraud Manual (Version 3) states that the use of FIRST is mandatory for everyone engaged in the investigation of fraud within the NHS.

5. What are the potential privacy impacts of this proposal?

Privacy impacts have been considered in the light of personal data gathered particularly in relation to alleged suspects. However this has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see section 4 of this document)

[4] http://www.nhsbsa.nhs.uk/Documents/Sect_1_-_B1_BSA_Directions_2013.pdf

6. Provide details of any previous PIA or other form of personal data* assessment done on this initiative (in whole or in part).

Full PIA completed in January 2017

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE – CONCLUSIONS

*IMPORTANT NOTE: 'Personal data' means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. (Data Protection Act, section 1)

PART 2 – DATA PROTECTION PRINCIPLES

DPA PRINCIPLE	SUB-SECTION	QUESTION	Y/N	RESPONSE
No.1 – Fair and Lawful Processing	**1.1 Preliminary** **Personal data shall be processed fairly and lawfully**	1. What type of personal data are you processing? Please give examples of any sensitive personal data that you are processing.	Y	Name of Subject ,Source, Witness Address of Subject , Source, Witness Contact details of Subject, Source, Witness Date of birth of Subject, Source, Witness Nationality and NI number of Subject. Passport Number of Subject. NHS Number of Subject Driving Licence Number of Subject. Payroll Number of Subject. Professional Body Subject registered to. Professional Registration Number of Subject. NHS Employment / links to NHS for subject Details of NHS Department to where subject may be attending for treatment. Detailed description of Subject. Bank details of Subject. Details of credit history and personal checks Vehicle details of Subject. Outcome relating to an offence for Subject Company Name (Non-NHS Subject only) SIC Code (Non-NHS Subject only) Registration Number (Non-NHS Subject only) Incorporation Date (Non-NHS Subject only) VAT Number (Non-NHS Subject only) Trading Address and Registered Address (Non-NHS Subject only Employment Information - Witness ***Sensitive Data as listed in Annex A*** **Commission or alleged commission of offences for Subjects.* **Proceedings relating to an actual or alleged offence for Subjects***.** **Racial or ethnic origin of Subject*

		2. Are sensitive personal data being differentiated from other forms of personal data? If yes, please specify procedures. If no, please indicate why not.	Y	NHS Protect protects information in a manner appropriate to its sensitivity, value, and criticality. As the combination of the entire dataset is a contribution to counter fraud investigations, the same robust security measures are therefore used regardless of the media on which information is stored within it, the systems which process it or the methods by which it is moved.
	1.2 Schedule 2 - Conditions relevant for purposes of the first principle: processing of any personal data	1. Have you identified all the categories of personal data that you will be processing and how? If yes, please list them. If no, please indicate why not.	Y	Details of the Source of information. Details of the Subject of the investigation. Details of any Witnesses in the investigation Details of the nature of the investigation
		2. Have you identified the purposes for which you will be processing personal data and how? If yes, please list them. If no, please indicate why not.	Y	The data is required for the following purposes: • Supporting fraud investigations by extracting and analysing data for individual cases • Developing processes to identify the scale of fraud • Applying knowledge from previous cases to identify further fraudulent activity • Identify irregular patterns which are indicative of fraud

		3. Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data? If yes, please list them. If no, please indicate why not.	Y	The processing is necessary under Schedule 2 • for the administration of justice, • for the exercise of any functions of the Crown, a Minister of the Crown or a government department, • for the exercise of any other functions of a public nature exercised in the public interest by any person.
		4. Are you relying on different grounds for different categories of personal data? If yes, how will this assessment be made?	N	N/A – it is all processed under the same grounds noted in Section X
	1.3 Schedule 3 - Conditions relevant for purposes of the first principle: processing of sensitive personal data If this project does not involve the processing of sensitive personal data, please go to section 1.4	1. Have you identified the categories of sensitive personal data that you will be processing? If yes, can you list them? If no, please indicate why not.	Y	Racial or ethnic origin of Subject Commission or alleged commission of offences Proceedings relating to an actual or alleged offence

		2. Have you identified the purposes for which you will be processing sensitive personal data? If yes, can you list them? If no, please indicate why not.	Y	The data is required for the following purposes: • Supporting fraud investigations by extracting and analysing data for individual cases • Developing processes to identify the scale of fraud • Applying knowledge from previous cases to identify further fraudulent activity • Identify irregular patterns which are indicative of fraud
		3. Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data? If yes, can you list them? If no, please indicate why not.	Y	The processing is necessary because of obligation from a minister of the crown that applies to NHS Protect as part of the Secretary of State directions (As detailed in the NHS Business Services Authority Directions 2013, schedule 1 part 9). The processing is disclosure of sensitive personal data by a person as a member of an anti-fraud organisation It would not be reasonable to obtain the consent of the data subject. The data is not established nor conducted for profit

		4. Are you relying on different grounds for different categories of sensitive personal data? If so, how will this assessment be made?	N	N/A
	1.4 Obtaining consent	1. Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2? If yes, when and how will that consent obtained?	N	No. It would not be reasonable to obtain the consent of the data subject.
		2. For the processing of sensitive personal data, are you relying on explicit consent as specified in Schedule 3, s1 of the Data Protection Act? If so, when and how will that consent obtained?	N	No. It would not be reasonable to obtain the consent of the data subject.
	1.5 Lawful processing	1. If you are a public sector organisation, does your processing of personal data fall within your statutory powers? If yes, please state what they will be. If no, please indicate why not.	Y	The processing is formalised via the Secretary of State directions to “obtain, monitor, collate and analyse such data held by any NHS body or local authority as the NHS Protect consider appropriate for the purposes of identifying trends and anomalies which may be indicative of fraud, corruption or other unlawful activities against or affecting the health service.” (As detailed in the NHS Business Services Authority Directions 2013 , schedule 1 part 9

		2. How is compliance with the Human Rights Act being assessed?	Y	The Information held within FIRST has been audited to ensure compliance with the Human Rights Act
		3. Are you assessing whether any of the personal data being processed is held under a duty of confidentiality? If yes, how will that assessment made? If no, please indicate why not.	Y	NHS Protect is fully compliant with the HMG Information Assurance Standard IS1 and IS2 standards The assessment of duty of confidentiality forms part of a Risk assessment conducted in accordance with these standards.
		4. How is that confidentiality maintained? (e.g. instructions on disclosure or shredding)	Y	NHS Protect Information Security Policy and Acceptable Use Policy covers all elements of appropriate behaviour with confidential information. NHS Protect staff are expected to follow these requirements and are subject to annual refresher training (with a subsequent examination)
		5. Are you assessing whether your processing is subject to any other legal or regulatory duties? If yes, how is that assessment being made? If no, please indicate why not.	Y	NHS Protect has an Information Governance and Risk Management Lead who is able to stay cognisant of legal issues and changes to the legalities of data user Yes. As part of this DPA Compliance Check and the related PIA this has been reviewed. Additionally, NHS Protect submits an annual IG Toolkit, in relation to the data captured and processed by the organisation, to demonstrate the NHS BSA policies and procedures it is managed in accordance with.

		6. How are you ensuring that those legal duties are being complied with?	Y	NHS Protect is audited annually against the ISO 27001 information standard (formally known as ISO/IEC 27001:2005) this is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
	1.6 Fair processing	1. Are individuals being made aware of the identity of your organisation as the data controller? If yes, state how they are being made aware. If no, please indicate why not.	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. It would be inappropriate for NHS Protect to advise individuals of the full extent of the purpose of their data being processed, as the purpose for doing so is to uncover fraudulent behaviour and therefore notification may result in the behaviours changing/becoming more complex and therefore harder to detect
		2. How are individuals being made aware of how their personal data is being used?	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. It would be inappropriate for NHS Protect to advise individuals of the full extent of the purpose of their data being processed, as the purpose for doing so is to uncover fraudulent behaviour and therefore notification may result in the behaviours changing/becoming more complex and therefore harder to detect

		3. How are individuals offered the opportunity to restrict processing for other purposes?	Y	This information is not processed for any other purposes.
		4. Do you receive information about individuals from third parties? If yes, please give examples. If no, please go to section 1.7	Y	Fraud information and evidence is gathered by NHS Protect from a variety of sources, information can be referred from the following organisations: NHS Health Bodies, NHS Foundation Trusts, Private Providers of NHS healthcare, NHS Commissioning Organisations. Department of Work and Pensions, Financial Institutions, Local Authorities, Media, NHS Source, Police Regulatory Bodies and Professional Bodies including (GMC) General Medical Council. (GOC) General Optical Council, (GPhC) General Pharmaceutical Council, (MHRA) Medicines and Healthcare Regulatory Agency. Additionally, member of the public are able to report concerns about fraud and corruption in the NHS by telephone to NHS Protect via the Fraud and Corruption Reporting Line (“FCRL”) and via an online (FCROL)

		5. How are individuals informed that the data controller is holding personal data about them?	Y	Individuals may request if the organisation holds personal information about them. Details are available on the BSA website on how to make this request.

	1.7 Exemptions from the first data protection principle The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller 2. the identify of any nominated data protection representative, where one has been appointed 3. the purpose(s) for which the data are intended to be processed 4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair Data Protection Act, Schedule 1, Part II, para. 2 (3)	1. Do you provide individuals with all of the information described in 1.7? If no, which exemption to these provisions is being relied upon?	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. As personally identifiable personal data captured by FIRST relates to individuals alleged to have been involved in fraudulent activity against the NHS. It would be inappropriate for NHS Protect to advise individuals of the full extent of the purpose of their data being processed, as the purpose for doing so is to uncover fraudulent behaviour and therefore notification may result in the behaviours changing/becoming more complex and therefore harder to detect. Data in relation to both the source and the witness is limited and has been provided by them voluntarily.

No.2 - THE PURPOSE OR PURPOSES FOR PROCESSING PERSONAL DATA Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	**2.1 Use of personal data within the organisation**	1. Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?	Y	Information Asset register and annual risk assessment.
		2. How often is this record checked?	Y	Every two months (prior to update of IT Security Forum.
		3. Does the record cover processing carried out on your behalf (e.g. by a subcontractor)?	Y	N/A - No processing is carried out on behalf of NHS Protect

		4. What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data? (Cross reference with section 1.6, Fair Processing)	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. It would be inappropriate for NHS Protect to advise individuals of the full extent of the purpose of their data being processed, as the purpose for doing so is to uncover fraudulent behaviour and therefore notification may result in the behaviours changing/becoming more complex and therefore harder to detect.
	2.2 Use of existing personal data for new purposes	1. Does the project involve the use of existing personal data for new purposes? If no, go to section 2.3	N	N/A
		2. How is the use of existing personal data for new purposes being communicated to:- (a) the data subject; (b) the person responsible for Notification within the organisation (c) the Information Commissioner?		N/A

		3. What checks are being made to ensure that further processing is not incompatible with its original purpose?		N/A
	2.3 Disclosure of data	1. Do you have a policy on disclosure of personal data within your organisation / to third parties? Is it documented?	Y	Contained within the Information Security Policy and Acceptable Use Policy
		2. How are staff made aware of this policy / instructed to make disclosures?	Y	Available on NHS Protect Intranet. Additionally, staff are expected to complete refresher training on a yearly basis (with subsequent examination) in relation to these principles.
		3. How are individuals / data subjects made aware of disclosures of their personal data?	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. It would be inappropriate for NHS Protect to advise individuals of the full extent of the purpose of their data being processed, as the purpose for doing so is to uncover fraudulent behaviour and therefore notification may result in the behaviours changing/becoming more complex and therefore harder to detect

		4. Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed? If no, go to section 3.1 If yes, how do you make the assessment?	Y	Requests must be made in writing, explaining the use of personal data being disclosed and information will only be disclosed once authorised by NHS Protect Data protection Officer. They would also be subject to the process for requesting personal data via written authorisation
No. 3 - ADEQUACY AND RELEVANCY	**3.1 Adequacy and relevance of personal data**	1. How is the adequacy of personal data for each purpose determined? (Please give examples.)	Y	By a) Identifying relevant datasets for each high risk area and assessing how Information Analytics could use this data and b) establishing normative behaviour to identify outliers against rules identified. The ability/inability to achieve the above forms part of the initial assessment of the data for the purposes of detecting fraudulent activity which will determine the continuation of the project and the subsequent data retention.
		2. How is an assessment made as to the relevance (i.e. no more than the minimum required) of personal data for the purpose for which it is collected? Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Y	This forms an integral part of the Privacy Impact Assessment that has been completed for this system.

		3. What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?	Y	This forms an integral part of the Privacy Impact Assessment that has been completed for this project.
		4. How often will these procedures reviewed?	Y	At any point at which the contents of the above document are deemed either out of date or no longer relevant due to changes to the data capture and outputs.
		5. Are there procedures for assessing the amount and type of personal data collected for a particular purpose? If yes, please describe. If no, please indicate why not.	Y	This forms an integral part of the Privacy Impact Assessment that has been completed for this project.
		6. Are items of personal data held in every case which are only relevant to a subset of those cases?	N	N/A

No. 4 - ACCURATE AND UP TO DATE Personal data shall be accurate and, where necessary, kept up to date.	**4.1 Accuracy of personal data**	1. How, and how often, are personal data checked for accuracy? Please give examples:	Y	Information is provided by individual NHS organisations from their own systems. Organisations are responsible for the accuracy of gathered data, for both their own records and additionally for information provided to us. Because NHS Protect has no means to audit or review this data for accuracy, it is accepted that this must be used with caution. Information which is subsequently used to support fraud investigations will be assessed against other records and forms of evidence for accuracy as part of the case management process for fraud investigations.
		2. Are personal data evaluated to establish the degree of damage to both the data subject / data controller that could be caused through inaccuracy?	Information which is subsequently used to support fraud investigations will be assessed against other records and forms of evidence for accuracy as part of the case management process for fraud investigations. Y	Damage cause by inaccuracy will be considered by the Crown Prosecution Service prior to progressing criminal case. Those identified after this point will be subject to the usual forms of compensation
		3. In what circumstances is the accuracy of the personal data being checked with the Data Subject? Please give examples:	Y	As part of the evidence gathering phase of a fraud investigation.

		4. Are the sources of personal data (i.e. data subject, data controller, or third party) identified in the record? If so, how? Please give examples:	Y	This will be clear from the NHS BSA data gathered and the organisation providing the NHS dental services providing it.
		5. Is there any facility to record notifications received from the data subject if they believe their data to be inaccurate? If no, please indicate why not.	Y	All request by the data subject are recorded by NHSP Data Protection Officer
	4.2 Keeping personal data up to date	1. Are there procedures to determine when and how often personal data requires updating?	N	There is no process possible by NHS Protect to determine when information should be updated, as there is no means to audit or review for accuracy – information is assumed accurate as provided (but caution is applied for use as a result)

		2. Are personal data evaluated to establish the degree of damage to: (a) the data subject or (b) the data controller that could be caused through being out of date? Please specify whether to data subject or data controller:	Y	Information which is subsequently used to support fraud investigations will be assessed against other records and forms of evidence for accuracy as part of the case management process for fraud investigations. Damage cause by inaccuracy will be considered by the Crown Prosecution Service prior to progressing criminal case. Those identified after this point will be subject to the usual forms of compensation
		3. Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?	Y	Information which is subsequently used to support fraud investigations will be assessed against other records and forms of evidence for accuracy as part of the case management process for fraud investigations.
No. 5 - NO LONGER THAN NECESSARY	**5.1 Retention policy**	1. What are the criteria for determining retention periods of personal data? How often are these criteria reviewed?	Y	This is documented in the NHS Protect Data Handling and Storage Policy currently in draft as of 28/07/17))
		2. Does the project(s) include the facility to set retention periods?	Y	This is a feature included in the process

		3. Is the project subject to any statutory / organisational requirements on retention? If yes, please state relevant requirements:	Y	Data will be retained only as long as necessary, up to a maximum period in accordance with the Data Protection Act 1998. The maximum period depends on whether fraudulent behaviour is detected – if fraud is found then the retention period is 7 Years, if fraud not found then its 3 years. The data will be stored in digital format and will be erased, using a CESG approved product (Blanco), from the relevant storage server when no longer required.
	5.2 Review and deletion of personal data	1. Is there a review policy and is it documented?	Y	Forms part of the NHSProtect Data Handling and Storage Policy

		2. When data is no longer necessary for the purposes for which it was collected: (a) How is a review made to determine whether the data should be deleted? (b) How often is the review conducted? (c) Who is responsible for determining the review? (d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?	Y	There is a deletion process in place, based on the age of the record. The maximum period depends on whether fraudulent behaviour is detected – if fraud is found then the retention period is 7 Years, if fraud not found then its 3 years. The data will be stored in digital format and will be erased, using a CESG approved product (Blanco), from the relevant storage server when no longer required. Audited annually as part of the impact assessment and RMADS of the System The FIRST Project Board addresses any unscheduled steps of archiving or removal of records The FIRST Project Board additionally makes a review at least annually in relation to the data being used. The system doesn't have an automatic facility to identify records due for removal and as such this is a manual process.
		4. Are there any exceptional circumstances for retaining certain data for longer than the normal period? If yes, please give justification:	N	No
		5. Is there any guidance on deletion / destruction of personal data? If no, please indicate why not.	Y	The NHS Protect Data Handling and Storage Policy (currently in draft) will provide descriptions of the process for removal of records.

No. 6 - SUBJECT ACCESS	**6.1 Subject access**	1. Are procedures in place to provide access to records under this Principle? If yes, please specify proposed procedures. If no, please indicate why not.	Y	There are processes in place for making a subject access request via the usual NHS BSA processes. The process for accessing the data for a subject access request would be the same for any other request (i.e. requiring written request, detailing the scope and extent of the personal info required and approval from the SRO prior to access to said data)
		2. How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?	Y	In order to identify an individual, enough data would be needed to a) confirm whether they exist within FIRST dataset and b) independently verify them should more than one individual be located with the same/similar details. Typically this will be a mix up surname and date of birth but may also be additionally filtered via a specific incident date, region or sector.
		3. Do you provide an explanation of any codes or other information likely to be unintelligible to a data subject? If yes, how? If no, please indicate why not	Y	Yes any codes and other information are explained to the data subject as part of the subject access request
		4. Are procedures in place to manage personal data relating to third parties? If yes, please specify proposed procedures. If no, please indicate why not?	Y	Limited Personal information in relation to the source and the witness is contained within the FIRST system and has been provided by them voluntarily. Given that these relate to fraud investigations and are alongside the personal data and sensitive personal data and are handled with the same security levels, this is deemed to have all risks mitigated.

		5. How is data relating to third parties managed?	Y	See Above
	6.2 Withholding of personal data in response to a subject access request	1. Are there any circumstances where you would withhold personal data from a subject access request? If no, go to section 6.3. If yes, on what grounds?	Y	Where exemptions allowable under section 7 of the DPA
		2. How are the grounds for doing so identified?	Y	Where this data is subject to inclusion in the detection of Fraud or as part of a fraud investigation
	6.3 Processing that may cause damage or distress	1. Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual? If yes, please specify proposed procedures. If no, please indicate why not.		Information which is subsequently used to support fraud investigations will be assessed against other records and forms of evidence for relevance as part of the case management process for fraud investigations. Damage/distress caused by inaccuracy will be considered by the Crown Prosecution Service prior to progressing criminal case. Those identified after this point will be subject to the usual forms of compensation
		2. Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?	Y	This will be included as part of the considerations.

	6.4 Right to object	1. Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?	N/A	N/A
	6.5 Automated decision-taking	1. Are any decisions affecting individuals made solely on processing by automatic means? If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?	N	No - There is no automatic decision making in the FIRST System
	6.6 Rectification, blocking, erasure and destruction	1. What is the procedure for responding to a data subject's notice (in respect of accessible records) or a court order requiring: (a) rectification; (b) blocking; (c) erasure or; (d) destruction of personal data?	Y	It is the responsibility of the Data Protection Officer to respond to any notices or court orders, however it would be feasible to locate records for this purpose if required. It is possible that it may be necessary to block any requests from the data subject on the grounds of section 7 of the DPA

No.7 - SECURITY OF PERSONAL DATA	**7.1 Security Policy**	1. Is there a Data Security Policy? If no, please indicate why not and then go to 7.1, question 5.	Y	
		2. If yes, who / which department(s) are responsible for drafting and enforcing the Data Security Policy within the organisation?	Y	NHS Protects Information Systems and Security Dept.
		3. Does the Data Security Policy specifically address data protection issues?	Y	
		4. What are the procedures for monitoring compliance with the Data Security Policy within the organisation?	Y	Regular Audit by CESG and the BSI for continued ISO 27001 certification. FIRST is also subject to internal and external audit
		5. Does the level of security that has been set take into account the state of technological development in security products and the cost of deploying or updating these?	Y	
		6. Is the level of security appropriate for the type of personal data processed?	Y	
		7. How does the level of security compare to industry standards, if any?	Y	Meets CESG requirements

	7.2 Unauthorised or unlawful processing of data	1. Describe security measures that are in place to prevent any unauthorised or unlawful processing of: (a) Data held in an automated format (e.g. password controlled access to PCs). (b) Data held in a manual record (e.g. locked filing cabinets)?	Y	Access to systems requires a password to access the system and all activity on the system is audited and monitored. Personal data is stored separately is encrypted upon receipt into the FIRST system. The data is decrypted when the server is started up and the decryption key entered by the Data Base Administrator. All off site back-ups are secure as they can only be opened via the encryption key. An additional level of data security is the Virtual Private Database (VPD) which automatically restricts access to cases once they are classified as confidential. A case can start off as restricted and be accessed by the LCFS and assigned NHSProtect staff. However if the classification of the case is upgraded to confidential then the LCFS would no longer be able to access. All FIRST personal data is stored electronic – no personal data should be in paper format beyond any immediate usage and disposal (should it prove necessary, the NHS BSA data confidentiality requirements for storing this data would apply). Users within FIRST are not able to access records apart from what they have submitted themselves or records to which they have been granted authorised access.

		2. Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing? If yes, please describe the planned procedures. If no, please indicate why not.	N	Personal data is stored separately is encrypted upon receipt into the FIRST system. The data is decrypted when the server is started up and the decryption key entered by the Data Base Administrator. All off site back-ups are secure as they can only be opened via the encryption key. An additional level of data security is the Virtual Private Database (VPD) which automatically restricts access to cases once they are classified as confidential. A case can start off as restricted and be accessed by the LCFS and assigned NHSProtect staff. However if the classification of the case is upgraded to confidential then the LCFS would no longer be able to access. NHS Protect protects information in a manner appropriate to its sensitivity, value, and criticality. As the combination of the entire dataset is a contribution to counter fraud investigations, the same robust security measures are therefore used regardless of the media on which information is stored within it. The systems which process it or the methods by which it is moved.

		3. Describe the procedures in place to detect breaches of security (remote, physical or logical)?	Y	Electronic: Next Generation approved firewalls and intrusion detection systems are installed. In addition to this NHS Protect have a log monitoring system in place to provide proactive SIEM monitoring. Physical: Swipe card access to the Data centre containing the FIRST system CCTV with 24/7 recording in the Data centre All FIRST IT Infrastructure in locked cabinets Remote & logical All FIRST activity monitored and audited. Protected by Firewalls and Intruder detection systems All security incidents logged with the Information Security Manager and Information Security Officer
	7.3 Destruction of personal data	1. Describe the procedures in place to ensure the destruction of personal data no longer necessary?	Y	It is the responsibility of the data protection officer to ensure destruction of personal data that is no longer necessary. The data will be stored in digital format and will be erased, using a CESG approved product (Blanco), from the relevant storage server when no longer required
		2. Are there different procedures for destroying sensitive personal data?	N	N/A

	7.5 Contingency planning - accidental loss, destruction, damage to personal data	1. Is there a contingency plan to manage the effect(s) of an unforeseen event?	Y	Business Continuity and Disaster Recovery plans are fully documented and up to date
		2. Describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through: • human error • computer virus • network failure • theft • fire • flood • other disaster.	Y	A full Business Continuity Plan (BCP) is in place and disaster recovery was successfully tested in November 2016. For further details see NHS Protect BCP, available from NHS Protect intranet.
	7.6 Choosing a data processor	1. What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?	N/A	The information is only processed by NHS Protect
		2. How did you assess their data security measures?	N/A	The information is only processed by NHS Protect
		3. How do you ensure that the Data Processor complies with these measures?	N/A	The information is only processed by NHS Protect

		4. Is there an on-going procedure for monitoring their data security measures? If yes, please describe. If no, please indicate why not.	N/A	The information is only processed by NHS Protect
No. 8 - OVERSEAS TRANSFER The European Economic Area (EEA) comprises the 27 EU member states plus Iceland, Liechtenstein and Norway. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	**8.1 Adequate levels of protection**	1. Are you transferring personal data to a country or territory outside of the EEA1? If no, please go to Part 3.	N	There is no transfer outside the EEA

		2. What are the types of data are transferred? (e.g. contact details, employee records)	N/A	
		3. Are sensitive personal data transferred abroad? If yes, please provide details:	N	
		4. What are the main risks involved in the transfer of personal data to countries outside the EEA?	N/A	There is no transfer outside the EEA
		5. Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?	N/A	There is no transfer outside the EEA
		6. Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?	N/A	There is no transfer outside the EEA
	8.2 Exempt transfers	1. Is your organisation carrying out any transfers of data where it has been decided that the Eighth Principle does not apply? If yes, what are they?	N	There is no transfer outside the EEA
		2. To which country / territory are these transfers made?	N/A	There is no transfer outside the EEA

		3. What are the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle? E.g. consent, (See DPA 1998, Schedule 4, for a full list)	N/A	There is no transfer outside the EEA

PART 3 – DATA PROTECTION PRINCIPLES (DPP) COMPLIANCE – CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

FIRST complies with the requirements of the Data Protection Act (DPA98).

_____ _____

(Proponent) (Data Protection Officer)

Date: _____ Date: _____