NHS
Counter Fraud Authority

AD LAB & Summation

Data Protection Impact Assessment

October 2018

V2.0

NHS fraud.
Spot it. Report it.
Together we stop it.

Executive Summary

This document contains information in relation to the AD LAB & Summation system used by the Forensic Computing Unit.

The system is a centralised forensic analysis platform to allow the processing, analysis and review of data recovered from digital devices submitted as part of NHS fraud investigations.

The system holds any data present on digital devices submitted to FCU for examination as part of criminal investigations

This document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (May 2018).
More information in relation to this data classification, including the requirements for working with these assets can be found here:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information 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 where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

Table of contents

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Susan Hyde	DPIA AD LAB & Summation	Trevor Duplessis	0.1 draft	11/09/2018	All – First Draft
Susan Hyde	DPIA AD LAB & Summation	Trevor Duplessis	0.2 draft	24/10/2018	Amendments to areas highlighted
Susan Hyde	DPIA AD LAB & Summation	Trevor Duplessis	0.3 for review	26/10/2018	All areas updated for final review
Susan Hyde	DPIA AD LAB & Summation	Trevor Duplessis	1:0 Final	05/11/2018	Final updates by FCUTL
Susan Hyde	DPIA AD LAB & Summation	Trevor Duplessis	2:0 Redacted	08/03/2019	Redacted prior to publication

Prefix	
Reference:	DPIA AD LAB & Summation
Date:	October 2018
Author:	Susan Hyde
Data Owner:	Richard Rippin
Version:	2:0
Supersedes	1:0

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	2018	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

1. Data Privacy Impact Assessment Requirement & Process

Introduction

1. The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.

2. DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.

3. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.

4. A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also affect other fundamental rights and interests:

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead **to physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy**, **unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data[1]…"

5. Under GDPR you must carry out a DPIA where for example you plan to:

- process special category or criminal offence data on a large scale.

6. The ICO also requires a DPIA to be undertaken for example, where you plan to:

- use new technologies;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

7. DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

[1] GDPR - Recital 75

8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

9. This DPIA is related to the NHSCFA RMADS, which outline the threats, risks and security countermeasures in detail. The RMADS was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

Name of Database /System General Description

10. AD LAB & Summation is a Centralised forensic analysis platform to allow the processing, analysis and review of data recovered from digital devices submitted as part of NHS fraud investigations.

11. The process involved in getting data into the system is as follows:

Exhibits are accepted into the FCU lab and recorded on the FCU case management system, Lima. This will include details on the type of exhibit, description, evidence bag seal number etc.

Exhibits are then examined using standard FCU operating procedures and where possible forensic images of each exhibit are created and securely stored on the FCU network storage system (StorNext). Forensic images are an exact copy of the original data held on the original device, stored in a proprietary format.
The resulting forensics images are then processed into the AD LAB platform using standard FCU operating procedures. This effectively populates the AD LAB database with the data held within each image.

Once processing has finished the data is made available for remote review through the Summation platform, This is a web based review tool and shares the same database as AD LAB. Control to this is strictly limited to only staff authorised to see it (e.g. FCU, case investigators)

Once the investigation team have finished the review any items required as evidence are exported by FCU and made available for the investigator to use, send to CPS etc. This exported data is held within StorNext and may also be held by the investigator on the NHSCFA corporate network within their own shared drives.

12. See above

13. For security and confidentiality purposes, the database is only accessible by CFA staff in NIS and also DHSC, CFS Scotland, CFS Wales, NHS England and LCFS investigators. Access is strictly controlled with user names and passwords and investigators only have access to their own specific cases. Only system admins have access to all cases and admin rights are restricted to FCU personnel only.

14. This is the only DPIA to be completed on the database and it has been carried out by the Information and Records Management Officer, in consultation with FCU Technical Lead and the Information Governance and Risk Management Lead.

15. AD LAB & Summation, in addition to GDPR is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

16. To ensure the Database/System meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template[2] comprised of seven steps:

Step 1 - Identify the need for a DPIA

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

Step 7 - Sign off and record outcomes

[2] Version 0.3 (20180209)

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
A Data Protection Impact Assessments was identified as being required for the AD LAB / Summation Database because of the personal data gathered. However as the data gathered is for the Investigation of fraud, the purpose is considered to be specific, justifiable and proportional. The system aims to provide the ability to investigate digital data held within forensic images in a Forensically sound and collaborative way. The system allows the date to be searched, filtered, examined and exported in a manner acceptable to producing evidence in a court of law.

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?

2. What is the source of the data?

3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

4. Why types of processing identified as 'likely high risk' are involved?

AD Lab is used to process forensic images of various types eg E01, AD1 etc. These are typically full bit for bit copies of the contents of a hard drive, memory stick, USB storage device etc or a logical forensic image (AD1 format) containing email data and documents supplied by NHS trusts.

Summation uses the same Database and accesses the same data as AD Lab and is simply used as a way for investigators to view the data via web browser.

Data is stored within the FCU network on dedicated storage platforms (Stornext) in both London and Newcastle. Data is only used in support of investigations and has been either seized lawfully or provided voluntarily.

Data is only shared with investigators and CPS as part of evidential case submissions and disclosure exercises

The data being processed can contain personal sensitive data and patient data.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?

2. How much data will you be collecting and using?

3. How often?

4. How long will you keep it?

5. How many individuals are affected?

6. What geographical area does it cover?

1. The data processed contains personal sensitive information for the purposes of investigating a Criminal offence and may include patient data
2. Impossible to say – changes for each case and depends on the exhibits submitted
3. As and when the investigation team require on a per case basis
4. Data is kept as per NHSCFA data retention policy – currently 6 years after case closed/appeal finished/POCA finished
5. Not possible to say
6. Potentially whole of UK – differs for each case

Describe the context of the processing:

1. What is the nature of your relationship with the individuals?

2. How much control will they have?

3. Would they expect you to use their data in this way

4. Do they include children or other vulnerable groups?

5. Are there any prior concerns over this type of processing or security flaws?

6. Is it novel in any way?

7. What is the current state to technology in this area?

8. Are they any current issues of public concern that you should factor in?

9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?

1. N/A
2. N/A
3. N/A
4. N/A
5. N/A
6. No, AccessData's Forensic products have been available in the UK for over 15 years and AccessData as a company have been working in the Data Collection & Forensic field for over 30 years.
7. The ADLAB & Summation software have existed for numerous years now and are regularly updated to support additional data types and provide new feature requests & fixes. We strive to have the latest version subject to testing and validation.
8. N/A
9. We are working towards ISO17025:2005 accreditation which we are on target to be granted by end of April 2019. As part of this we work to the Forensic Science Regulators Code of Conduct and follow the ACPO Good Practice Guide for Digital Evidence.

Describe the purposes of the processing:

1. What do you intend to achieve?

2. What is the intended effect on individuals?

3. What are the benefits of the processing, for you and more broadly?

Support of investigations – without this data processing it would render investigators unable to carry out their role and responsibilities/
The processing is imperative to locate evidence and also locate material which would assist the defence or undermine a prosecution.
The FCU processes this data so that it is handled forensically by suitably trained & competent staff, ensuring the integrity of the data is maintained and available to be produced evidentially for court when necessary.

STEP 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

2. Who else do you need to involve within your organisation?

3. Do you need to ask your processors to assist?

4. Do you plan to consult information security experts or any other experts?

Ideally, DPIAs 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.

As such, this section is not applicable as it relates to new projects only and the AD LAB & Summation Database is already in use.

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?

2. Does the processing actually achieve your purpose?

3. Is there another way to achieve the same outcome?

4. How will you prevent function creep?

5. How will you ensure data quality and data minimisation?

6. What information will you give individuals?

7. How will you help to support their rights?

8. What measures do you take to ensure processors comply?

9. How do you safeguard any international transfers?

1. Data has been obtained either by lawful seizure under PACE/Search Warrant or provided voluntarily or by way of a DPA request.
   Processing is lawful under GDPR Article 6 (1)(e)Public Task
2. Yes this achieves our purpose. Processing/searching/storing is the only way to support the investigations which the data relates to.
3. No
4. N/A
5. The data is processed and searched under strict paramaters provided by the investigators. We do not work outside these parameters.
6. N/A
7. N/A
8. N/A
9. N/A

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant, or Severe	**Overall risk** Low, Medium or High
As a result of an attack on the NHSCFA network, personal or patient data held by FCU could be stolen or leaked. However this is unlikely due to existing IT security measures in place to protect the NHSCFA and FCU networks.	Remote	Significant	Low

STEP 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.	**Effect on risk** Eliminated, Reduced, Accepted	**Residual risk** Low, Medium, High	**Measure approved** Yes/No
Additional measures already taken involve separating the FCU network from the main corporate network so it is not presented to the internet. IT Security & Firewalls in place to prevent access.	Reduced & Accepted	Medium	Yes

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Trevor Duplessis DPO 22.03.19	If your decision departs from individuals' view, you must explain your reasons
Comments: I am satisfied that a comprehensive assessment of the system has been undertaken. Access is strictly controlled with user names and passwords and investigators only have access to their own specific cases, thereby making it fully auditable. Only system admins have access to all cases and admin rights are restricted to FCU personnel only. AD LAB & Summation does not have any direct interconnections with other NHSCFA systems or applications. Backups of the system are done to tape internally at each site. Copies of forensic images are kept offsite with Restore in a physically locked (4 digit combination lock) turtle case and stored on tape in a proprietary format.		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Ownership

16. The following table describes the AD LAB & Summation roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Richard Rippin
Senior Responsible Officer (SRO)	Richard Hampton
Application/Database Owner	Gareth Ballance
Data Protection Officer	Trevor Duplessis

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

10. AD LAB & Summation is a Centralised forensic analysis platform to allow the processing, analysis and review of data recovered from digital devices submitted as part of NHS fraud investigations.
11. The system holds any data present on digital devices submitted to FCU for examination as part of criminal investigations
12. The impact level of the AD LAB & Summation Database was assessed as CONFIDENTIAL and it can only be accessed internally.
13. The following measures briefly describe what controls have been implemented to protect the AD LAB Database and the personal data recorded:
    a. Backups of the database are not kept off-site but are backed up to tape internally at each site. Copies of forensic images are kept offsite with Restore in a physically locked (4 digit combination lock) turtle case and stored on tape in a proprietary format
    b. The system is only accessible by CFA staff in NIS and also DHSC, CFS Scotland, CFS Wales and LCFS investigators. Access is strictly controlled with user names and passwords and investigators only have access to their own specific cases. Only system admins have access to all cases and admin rights are restricted to FCU personnel only
    c. AD LAB & Summation does not have any direct interconnections with other NHSCFA systems and applications
    d. The Data Custodian must comply with the data protection requirements 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 NHSCFA register and the NHSCFA DPO is aware of its existence.
14. It is assessed that there are no residual privacy risks to the personal data used by the AD LAB & Summation Database.

15. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

16. Describe the purpose of the System.

AD LAB & Summation is a centralised forensic analysis platform to allow the processing, analysis and review of data recovered from digital devices submitted as part of NHS fraud investigations

17. Who has responsibility for the administration of the system.

The Forensic Computing Unit (FCU) is responsible for the administration of the system.

18. The information has been saved from a storage device or computer seized for analysis, and subsequently transferred to the system. As such it could include any type of personal data as categorised in Annex A of this DPIA. As we do not know what data is available for analysis until the information is received and transferred, the list would be non exhaustive.

19. The same applies for or sensitive personal data.

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

a. For security and confidentiality purposes, the database is only accessible by NIS, DHSC, CFS Scotland, CFS Wales and LCFS investigators. Access is strictly controlled with user names and passwords and investigators only have access to their own specific cases. Only system admins have access to all cases and admin rights are restricted to FCU personnel only

b. The system does not have a direct interconnection with other NHSCFA systems or applications

c. The IAO must comply with data protection requirements. 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. The AD LAB / Summation Database is subject to NHSCFA Data Handling and Storage Policy, currently 6 years after case closed/appeal finished/POCA finished

There are no paper records, FCU has its own control of records policy which is aligned with the NHSCFA policy

13. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

14. For security and confidentiality purposes, the database is only accessible by CFA Internal staff in NIS, and also DHSC, CFS Scotland, CFS Wales and LCFS investigators. Access is strictly controlled with user names and passwords and investigators only have access to their own specific cases. Only system admins have access to all cases and admin rights are restricted to FCU personnel only.

Section 5: External Sharing and Disclosure of Data

15. Information is shared with the investigators office that have responsibility for the case, this could be police, LCFS's, CFS Scotland investigators etc.

Section 6: Notice/Signage

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

NHSCFA's privacy policy on its website hosts separate sections in relation to data collection, retention and storage. This broadly covers all elements of the NHSCFA usage of data, in a nonspecific manner.

17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this Database and therefore outside the scope of this DPIA.

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

18. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

19. It is unlikely that many access requests will be received as the personal data recorded is in relation to fraud investigations, and as such are confidential until such point they are substantiated.

20. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

21. 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

22. The security and technical access architecture of the ADLAB & Summation Database is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official-Sensitive** and the hosting infrastructure is subject to CESG approved IT Security Health Check.

23. For security and confidentiality purposes, the database is only accessible by CFA Internal staff from NIS, and also DHSC, CFS Scotland, CFS Wales and LCFS investigators. Access is strictly controlled with user names and passwords and investigators only have access to their own specific cases. Only system admins have access to all cases and admin rights are restricted to FCU personnel only

24. The technical controls to protect the database include:

a. Anti-virus protection;

b. Permission based access controls

c. Audit logs if required

d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

25. The Database/System holds personal information taken both by telephone and electronically and is located at both Newcastle and London NHS Counter Fraud Authority sites.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the AD LAB / Summation Database, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

a. The GDPR and 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 NHSCFA security policy.

4. The Database/System processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, see Annex C *[delete / amend accordingly]*

The Privacy and Electronic Communications Regulations

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

Conclusion

8. There are no residual privacy risks to the personal data recorded in the Database/System. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

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 GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. 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 within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

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

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA
Project	AD LAB & Summation

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 DPIA)

Name, Title	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, NHSCFA
Phone Number	020 7895 4642
E-Mail	Trevor.Duplessis@nhscfa.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.

Centralised forensic analysis platform to allow the processing, analysis and review of data recovered from digital devices submitted as part of NHS fraud investigations

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

NHSCFA leads on a wide range of work to protect NHS staff from economic crime.

The purpose of the Database/System is: to allow the processing, analysis and review of data recovered from digital devices submitted as part of NHS fraud investigations.

For security and confidentiality purposes, the database is only accessible by Internal staff within NIS and also DHSC, CFS Scotland, CFS Wales and LCFS investigators. Access is strictly controlled with user names and passwords and investigators only have access to their own specific cases. Only system admins have access to all cases and admin rights are restricted to FCU personnel only

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

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the AD LAB / Summation Database 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 Compliance Checks in section 3 of this document)

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

This is the first DPIA carried out on the system

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.

Page left intentionally blank.

NHSCFA offices

Coventry

Cheylesmore House
5 Quinton Road
Coventry
West Midlands
CV1 2WT

02476 245500

London

4th Floor
Skipton House
80 London Road
London
SE1 6LH

0207 895 4500

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH

0191 204 6303