

OFFICIAL



Counter Fraud Authority

ALTIA Investigation Toolkit

Data Protection Impact Assessment

August 2023

V1.0 Published



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

OFFICIAL

Executive Summary

This document contains information in relation to ALTIA Investigation Toolkit.

The 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 (June 2023)

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

[Government Security Classifications Policy June 2023.docx \(publishing.service.gov.uk\)](#)

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'**

The document is subject to CROWN COPYRIGHT. It is provided in confidence under existing laws, regulations and agreements relating to the protection of data and shall be so protected. The information contained herein is proprietary and shall only be used for the purposes intended at release. It shall not be reproduced, adapted or used in, whole or in part, for any other purpose without the prior written consent of the Secretary of State for DEPT in the Government of the United Kingdom.

Nothing contained herein should be construed as endorsing any particular Technical Solution to any United Kingdom Government Invitation to Tender.

OFFICIAL

2

Table of contents

Executive Summary 2

Links & Dependencies..... 5

1. Data Protection Impact Assessment Requirement & Process 6

Introduction 6

ALTIA Investigation Toolkit - General Description..... 7

 Data Protection Impact Assessment..... 7

 Ownership 18

2. DPIA Report..... 18

 Section 1: Data Maintenance and Protection Overview 18

 Section 2: Uses of the Application and the Data 18

 Section 3: Data Retention 19

 Section 4: Internal Sharing and Disclosure of Data 19

 Section 5: External Sharing and Disclosure of Data 19

 Section 6: Notice/Signage 19

 Section 7: Rights of Individuals to Access, Redress and Correct Data 19

 Section 8: Technical Access and Security 20

 Section 9: Technology 20

3. Compliance Checks..... 20

 DPA 2018 Compliance Check 20

 The Privacy and Electronic Communications Regulations 21

5. The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes. 21

 The Human Rights Act 21

 The Freedom of Information Act 21

 Conclusion 21

Annex A - Definition of Protected Personal Data..... 22

Annex B - Data Protection Compliance Check Sheet..... 23

OFFICIAL

Document Control					
PM	Ref	Document owner	Version No	Issue Date	Amendments
Financial Investigation & Intelligence Lead	DPIA ALTIA Investigation Toolkit	DPO	V0.1	June 2023	Initial creation
Financial Investigation & Intelligence Lead	DPIA ALTIA Investigation Toolkit	DPO	V1.0	August 2023	Final version Published

Prefix	
Reference:	DPIA ALTIA Investigation Toolkit
Date:	August 2023
Author:	Financial Investigation & Intelligence Lead
Data Owner:	Financial Investigation & Intelligence Unit
Version:	1.0
Supersedes	N/A

OFFICIAL

OFFICIAL

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	June 2023	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
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
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

OFFICIAL

1. Data Protection 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:
 - a. "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 data¹..."
5. Under GDPR you must carry out a DPIA where for example you plan to:
 - a. 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:
 - a. use new technologies;
 - b. match data or combine datasets from different sources;
 - c. 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

OFFICIAL

1. 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**
8. This DPIA is related to the NHSCFA Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

ALTIA Investigation Toolkit - General Description

9. The purpose of the Altia Investigation Toolkit is: to provide a set of templates to apply to data, making analysing and visualising complicated financial information simple, efficient and powerful. It can quickly ingest, analyse, visualise and then rapidly act on usable information. The ALTIA investigation Toolkit is a piece of software made available to apply templates to bank statements / credit card statements and the like obtained via Crown Court Production Order, in order that the data contained within those financial statements becomes easily and quickly interpreted.
Access is restricted to approximately 10 members of staff within NHSCFA, including the database administrators
10. The data is collected in the form of bank account statements from financial institutions, in its raw form as provided by the relevant financial institution; it is then used in the ALTIA Investigation Toolkit to process it into Excel spreadsheets in order that it can be read and understood more easily.
11. This is the first DPIA to be completed on the system and it has been carried out by the Information and Records Management Officer, in consultation with Financial Investigation & Intelligence and the Information Governance and Risk Management Lead.
12. The Altia Investigation Toolkit, 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

13. To ensure the Altia Financial Analysis Toolbar 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 template² 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.

Investigation Toolkit provides a set of templates to apply to data, making analysing and visualising complicated financial information simple, efficient and powerful. It can quickly ingest, analyse, visualise and then rapidly act on usable information. The ALTIA investigation Toolkit is a piece of software made available to apply templates to bank statements / credit card statements and the like obtained via Crown Court Production Order, in order that the data contained within those financial statements becomes easily and quickly interpreted.

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?

1. The data in the form of bank account statements from financial institutions is collected in its raw form as provided by the relevant financial institution; it is then used in the ALTIA Investigation Toolkit to process it into Excel spreadsheets in order that it can be read and understood more easily. The raw data and ALTIA processed material is then stored in the Clue case management system with restrictions on who is able to view and access, with copies stored in a secure Financial Investigation folder on Teams

2. The source of the data is the relevant financial institution

3. The data is shared initially with the Officer in Charge of the relevant criminal investigation, but it would also possibly eventually be shared in a redacted format with CPS, Defence Barristers and a Court of Law

4. The data being processed is personal financial information, including, name, personal and banking address, account/card numbers, spending & income history

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?

2. The nature of the data is personal financial information, obtained via Crown Court Production Order for use in the investigation of criminal offences such as fraud, bribery and money laundering.
3. Difficult to quantify, however could be multiple bank accounts and credit card statements for example.
4. Weekly / monthly basis – regularly.
5. The data retention period is 6 years
6. Multiple.
7. UK -wide – predominantly England.

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 there 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. None, they are usually suspects in a criminal investigation.
2. None, unless they have voluntarily consented to provide personal banking information.
3. Unlikely, again unless they had voluntarily consented to divulge their personal banking information.
4. Not usually.
5. No.
6. No.
7. It is a system widely employed in the Law Enforcement arena.
8. No.
9. The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network.

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?

1. To be able to process raw format banking material into easily readable and analytically based excel spreadsheets.
2. None, other than to make this personal banking information easier to understand, see patterns, provide evidence of offending etc.
3. To enable evidence to be easily adduced of offending such as fraud, money laundering and bribery.

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?

1. Not applicable to do so, given this processing is done as part of a criminal investigation.
2. Only those involved in the criminal investigation process need to be involved.
3. Training is often provided on a as required basis, particularly around any updates to the software capabilities.
4. No

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

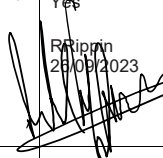
1. What is your lawful basis for processing?
2. Does the processing actually achieve your purpose?
3. Is there another way to achieve the same outcome?
4. How will you prevent function creep?
5. How will you ensure data quality and data minimisation?
6. What information will you give individuals?
7. 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. Consent and public task.
2. Yes.
3. No other software available to achieve this processing task.
4. The capability of the software is fixed barring any function enhancements.
5. Take the risk of human error out of forensically analysing financial and documentary evidence. Automatically sort, count, total or average financial data without human intervention, before summarising complex data quickly and creating custom reports and lists. Ensure consistency and thoroughness in every investigation or intelligence probe.
6. Information only given in the context of the investigation as required.
7. Personal data kept protected to limited relevant user group on Clue management system and within access controlled financial investigation folder on Teams.
8. Processors are given the appropriate training in the use of the software and its subsequent use and storage on Clue and Teams.
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
Unauthorised access to, or use of sensitive personal information obtained for lawful investigative purpose.	Possible	Significant	Low
Inappropriate accidental disclosure	Remote	Significant	Low
Inappropriate retention of duplicate data saved in different locations	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	Residual risk	Measure approved by SMT Owner
Ensure access to data is kept to minimum – secure storage on Clue and Teams.	Eliminated, Reduced, Accepted	Low, Medium, High	Yes 

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by SMT Owner:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by SMT Owner:		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
<p>Comments:</p> <p>Having reviewed the DPIA I am satisfied that a comprehensive assessment of the Toolkit has been carried out. Use of the Toolkit will be limited to approximately 10 members of staff including IT administrators.</p> <p>The primary purpose of the Toolkit is to convert information contained within banking documentation such as bank statements and convert them into a spreadsheet format. Once converted the data is exported from the Toolkit to a folder within the Microsoft TEAMS application. The Toolkit does not retain hold any personal data following export.</p> <p>All data processed is governed in accordance with current legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the with the organisational security measures employed.</p>		
Consultation responses reviewed by:	Trevor Duplessis - 17 th August 2023	If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by the Information and Records Management Officer:		The DPO should also review ongoing compliance with DPIA

Ownership

The following table describes the roles and responsibilities

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	National Operations Manager
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Financial Investigation & Intelligence Lead
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The impact level of the ALTIA Investigation Toolkit was assessed as OFFICIAL SENSITIVE and it can only be accessed internally.
2. The following measures briefly describe what controls have been implemented to protect the ALTIA Investigation Toolkit and the personal data recorded:
 - a. Altia Financial Toolkit is accessed by approximately 10 members of staff from NHSCFA, which includes the database administrator
 - b. Altia Financial Toolkit does not have any direct interconnections with other NHSCFA systems and applications
 - c. 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.
3. It is assessed that there are no residual privacy risks to the personal data used by the ALTIA Investigation Toolkit.
4. 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

5. The Financial Investigation & Intelligence Lead has responsibility for the administration of the Toolkit.
6. Information in the Database/System could include; Personal data including financial transactions, bank account details, possible third party information.

OFFICIAL

7. No sensitive data is processed. – data is processed as listed above.

8. 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

9. Altia Investigation Toolkit is subject to NHSCFA Data Handling and Storage Policy. Altia does not retain data, and any data saved in folders, will be deleted manually after 6 years.

10. 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

11. The Database/System is accessed by approximately 10 members of staff from NHSCFA, and includes 1 database administrator

Section 5: External Sharing and Disclosure of Data

12. The data is shared initially with the Officer in Charge of the relevant criminal investigation, but it would also possibly eventually be shared in a redacted format with CPS, Defence Barristers and a Court of Law

Section 6: Notice/Signage

13. Data subject will be aware during the course of the investigation that we hold data for them.

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.

14. 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/System and therefore outside the scope of this DPIA.

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

15. 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.

16. It is unlikely that many access requests will be received as the personal data recorded is all in relation to criminal investigations.

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

18. 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

19. The security and technical access architecture of the toolkit is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official**, and the hosting infrastructure is subject to the ISO27000 and ISO27001

20. Access is restricted to internal staff only.

21. The technical controls to protect the database include:

- a. Anti-virus protection;
- b. Permission based access controls to shared drive.
- c. Logging, audit and monitoring [controls].
- d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

22. The Database/System holds personal information obtained electronically and is located in the NHS Counter Fraud Authority data centre.

Commented [SH1]: Is there a facility within Altia to monitor who is logged on? If not - this line can be removed.

Commented [SW2R1]: No.

Commented [TD3R1]: So the only access control would be ISA's record of who has access to the toolkit?

Commented [SW4R1]: Correct.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the Toolkit, 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 Altia Financial Toolkit does not process sensitive personal data.

OFFICIAL

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 Altia Financial Toolkit. 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.

OFFICIAL

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 NIS
Project	Altia – Financial Investigation Toolkit

2. Contact position and/or name

(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Trevor Duplessis
Branch / Division	Corporate Affairs, NHSCFA

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.

ALTIA Investigation Toolkit

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 Altia Investigation Toolkit is: to provide a set of templates to apply to data, making analysing and visualising complicated financial information simple, efficient and powerful. It can quickly ingest, analyse, visualise and then rapidly act on usable information. The ALTIA investigation Toolkit is a piece of software made available to apply templates to bank statements / credit card statements and the like obtained via Crown Court Production Order, in order that the data contained within those financial statements becomes easily and quickly interpreted.

Access is restricted to approximately 10 members of staff within NHSCFA, including the database administrators.

OFFICIAL

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 ALTIA Investigation Toolkit Database/System 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.

OFFICIAL

OFFICIAL

Page left intentionally blank.

NHSCFA offices

Coventry

9th Floor
Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

7th Floor
10 South Colonnade
Canary Wharf
London
E14 4PU

Newcastle

1st Floor
One Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH

OFFICIAL