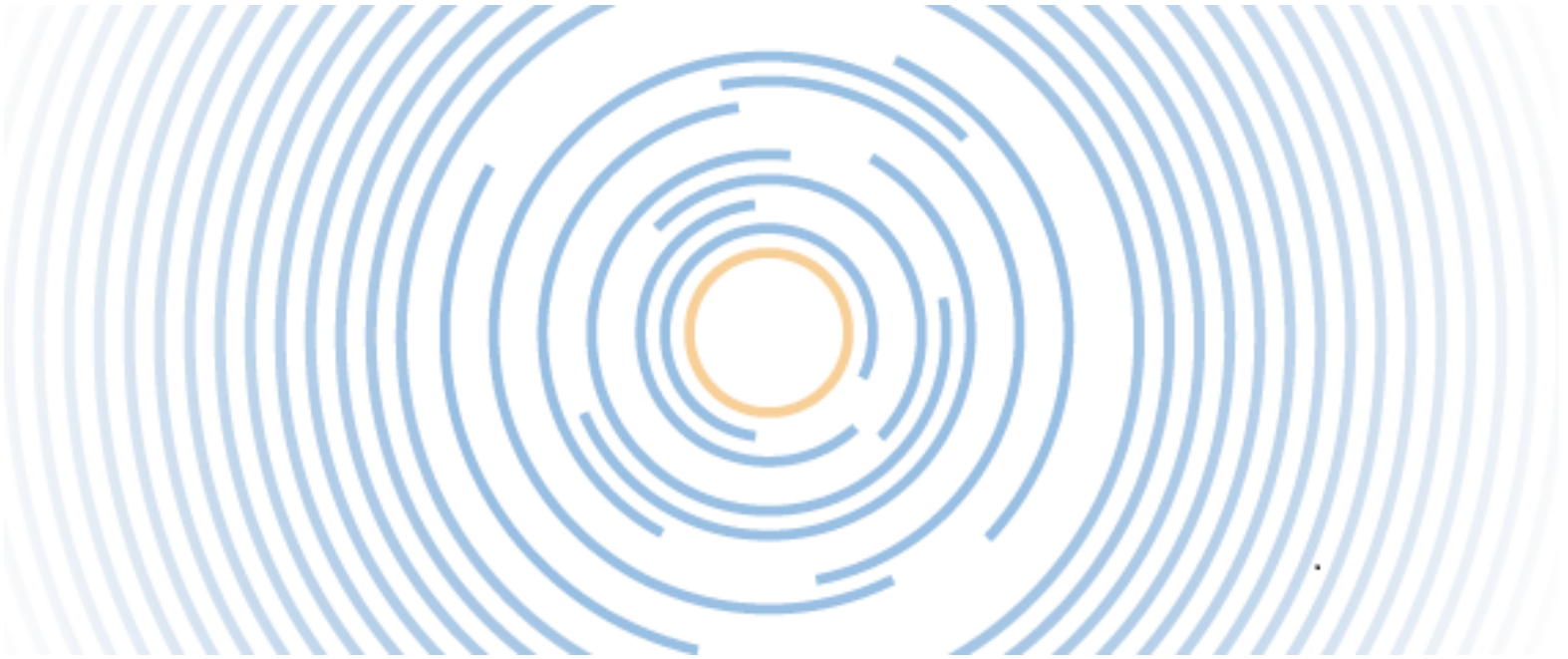
NHS Protect

Lima Portal and Forensic Case Management System

Privacy Impact Assessment

V2.1 Published

October 2017



Executive summary

This document contains information in relation to the Lima Portal and Forensic Case Management System.

Lima Forensic Case Management Software from IntaForensics is a complete, end-to-end case management system that offers an easy way to organise every aspect of a digital forensic investigation. The standout feature for Lima is its ability to tailor the system to the needs of the organisation. Lima provides enough functionality and customization capabilities to meet demand.

The system can be used to establish case management procedures that follow industry regulations, legal requirements and digital forensic best practices. This will help to ensure that if a case goes to court, or the process is audited by a regulatory agency, that there is a defensible and repeatable process in place. Additionally, Lima provides some out-of-the-box functionality that can be useful. It can be configured to use an SMTP server, allowing alert and update emails to be sent to designated users throughout an investigation.
Lima also allows the use of custom-report templates. These can be populated at the click of a button with data from the case in those instances where a physical document needs to be produced.

The Lima Forensic Case Management System adapted for use by NHS Protect contains all information in relation forensic investigations, contemporaneous notes as well as acquisition and analysis information. It also stores requests from officers in charge of the fraud investigation as an automatic transfer from the Lima Portal. As such the document is deemed OFFICAL.
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'

Table of contents

Table of contents 3
Links & Dependencies 5
Table 1 – Links and Dependencies 5
Section 1: 6
Privacy Impact Assessment Requirement & Process 6
Introduction 6
PIA Phases 6
Lima General Description 7
Ownership 8
Section 2: PIA Screening 8
The PIA Screening Process 8
Screening Process Conclusions 14
Section 3: PIA Report 15
Section 4: Compliance Checks 19
DPA 98 Compliance Check 19
The Privacy and Electronic Communications Regulations 19
The Human Rights Act 1998 19
The Freedom of Information Act 19
Annex A - Definition of Protected Personal Data 20
Annex B – Lima Personal Data 21
Annex C – Data Protection Compliance Check Sheet 22

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Information and Records Management Officer	**PIA / Lima Portal and Forensic Case Management System**	**DPO**	**V0.1**	**10/10/2017**	**All**
Information and Records Management Officer	**PIA / Lima Portal and Forensic Case Management System**	**DPO**	**V0.2**	**01/11/2017**	**Final comments from Data Protection Officer and Application Owner**
Information and Records Management Officer	**PIA / Lima Portal and Forensic Case Management System**	**DPO**	**V1.0**	**22/05/2019**	**Reviewed and prepared for publication – no redactions or amendments to original**
Information and Records Management Officer	**PIA / Lima Portal and Forensic Case Management System**	**DPO**	**V2.0**	**13/09/2021**	**Reviewed and anonymised for final publication – no amendments to original version completed in 2017**
Information and Records Management Officer	**PIA / Lima Portal and Forensic Case Management System**	**DPO**	**V2.1**	**14/02/2023**	**No amendments *addendum to original version completed in 2017.**

Page No's	14**.02.2023: Addendum**
5	Links and Dependencies – Reference to Data Protection Act 2018 added

Prefix	
Reference:	**PIA/Lima Portal and Forensic Case Management System**
Date:	**October 2017 (Original completion date)**
Author:	**Information and Records Management Officer**
Data Owner:	**Head of Operations**
Version:	**2.1**
Supersedes	**2.0**

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	1998 (Revised Act 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	April 2014	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
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
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

Table 1 – Links and Dependencies

Section 1:

Privacy Impact Assessment Requirement & Process

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 that process or store personal data on more than 250 people will require a PIA to be conducted and documented as part of the accreditation evidence.

2. 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. It enables organisations to anticipate 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. 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.

4. This PIA is related to the NHS PROTECT RMADS, which outline the threats, risks and security countermeasures in detail. The RMADS was developed in accordance with the requirements of NHS Protect and CESG HMG Infosec Standards 1 and 2.

PIA Phases

5. 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.

Lima Portal and Forensic Case Management System

General Description

6. Lima Forensic Case Management Software from IntaForensics is a complete, end-to-end case management system that offers an easy way to organise every aspect of a digital forensic investigation. The standout feature for Lima is its ability to tailor the system to the needs of the organisation. Lima provides enough functionality and customisation capabilities to meet demand.
The system can be used to establish case management procedures that follow industry regulations, legal requirements and digital forensic best practices. This will help to ensure that if a case goes to court, or the process is audited by a regulatory agency, that there is a defensible and repeatable process in place. Additionally, Lima provides some out-of-the-box functionality that can be useful. It can be configured to use an SMTP server, allowing alert and update emails to be sent to designated users throughout an investigation.

   Lima also allows the use of custom-report templates. These can be populated at the click of a button with data from the case in those instances where a physical document needs to be produced.
The Lima Forensic Case Management System adapted for use by NHS Protect contains all information in relation forensic investigations relating to allegations of fraud, bribery and corruption within the NHS. It holds contemporaneous notes as well as acquisition and analysis information and also stores requests from officers in charge of the fraud investigation as an automatic transfer from the Lima Portal.

7. The system has been used by the NHS Protect Forensic Computing Unit since 2010 as a means of managing requests and information in relation to forensic investigations. Requests for forensic investigations including related information are also received from external Local Counter Fraud Specialists (LCFS) in Scotland, Counter Fraud Wales, the police force, HMRC and DH.

8. Cases are submitted to the Forensic Computing Unit (FCU) via Lima portal or via a Case Submission form (if from an external body which does not have Lima Portal access). The FCU assesses the cases and if accepted exhibits will then be delivered to FCU for examination or if the request is to assist on-site, FCU will attend premises with investigation teams and undertake examinations and forensic imaging on-site. Details about items being examined and the equipment used to examine them is recorded within Lima as are contemporaneous notes and other actions that the Computer Forensic Specialist carries out. Once forensic images have been created these are processed using specialist forensic software and then searched using criteria provided by the OIC/Investigation team. The results of the processing and searching are made available for review by the investigators and once items relevant to the case are identified FCU produce a report containing these items. FCU will also write statements for court when required and will attend to give live evidence during trial if needed.

9. For security and confidentiality purposes, access to the Lima Forensic Case Management System is restricted to five members of staff from the Forensic Computing Unit as well as read only access to the FCU manager and 2 NHS Protect internal auditors, whilst approximately 30 staff from the National Investigations Service have access to their own authorised area of the Lima Portal that links directly to the system.

10. The Lima Portal and Forensic Case Management System, 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 it 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

The following table describes the Lima Portal and Forensic Case Management System roles and responsibilities:

Role	Responsibility
Information Asset Owner (IAO)	Head of Operations
Senior Responsible Officer (SRO)	Head of Intelligence and Crime Reduction
Application Owner	FCU Technical Lead
Data Protection Officer	Information Governance and 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.

4. This is the only Privacy Impact Assessment to be completed on the system and it has been carried out by the Information and Records Management Officer, in consultation with the Information Governance and Risk management Lead.

Ser	Question	Response
1	System/Application/Project Name	Lima
2	What is the main function of the System/Application/Project?	The Lima Forensic Case Management System is a piece of software from IntaForensics, and a complete end to end case management system to organise every aspect of a digital forensic investigation. The system contains all information in relation to forensic investigations, contemporaneous notes as well as acquisition and analysis information. It also stores requests from officers in charge of the case as an automatic transfer from the Lima Portal.
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.
4	What [1]personal data is collected? (See Annex A for definitions)	The following personal data is captured by the Lima Portal and Forensic Case Management System, **NB This is not an exhaustive list ..please see Annex A of PIA** Name, address & contact details, date of birth. Nationality, NI number & Passport Number. NHS Number, Driving Licence Number Payroll Number of Subject. Professional Body Subject registered to. Professional Registration Number NHS Employment / links to NHS Details of NHS Department to where subject may be attending for treatment. Detailed description. Bank details. Details of credit history and personal checks Vehicle details. 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 ***Sensitive Data as listed in Annex A of PIA*** **Commission or alleged commission of offences for Subjects.* **Proceedings relating to an actual or alleged offence for Subjects***.** **Racial or ethnic origin of Subject*

[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?	The personal data is provided by Senior Fraud Investigators from NHS Protect, external Local Counter Fraud Specialists (LCFS) in Scotland, Counter Fraud Wales, the police force, HMRC and DH. External work requests are received via a submission form, emailed directly to Forensics and saved in the relevant FCU stornext share (secure folder).
6	Why is the personal data being collected?	The data is collected in order for a forensic investigation to be conducted.
7	How is the personal data collected?	Information is collected from NHS Protect Investigators as an automatic transfer from the Lima Portal to the Lima Forensic Case Management System, having initially originated from an investigation on FIRST (Fraud Investigation Reporting System Toolkit) Information is also collected from external Local Counter Fraud Specialists (LCFS) in Scotland, Counter Fraud Wales, the police force, HMRC and DH following completion of a request for work form. Submission forms in respect of external requests are emailed to the forensics team, where they are saved within the relevant case folder on the relevant FCU stornext share (i.e either London or Newcastle). The case overview, remit and suspect information will be copied into the Lima case created for this submission. All exhibit details will also be created within the Lima case either at the point of receiving them or before they are delivered.
8	Describe all the uses for the personal data (including for test purposes).	The data is used to understand the subject of a forensic investigation and to conduct keyword searches. It would not be used for test purposes.
9	Does the system analyse the personal data to assist Users in identifying previously unknown areas of note, concern or pattern?	The system does not analyse the personal data, it only stores it. Any searches would be carried out by a system called Access Data Labs.
10	Is the personal data shared within internal organisations?	Access to the Lima Forensic Case Management System is restricted to five members of staff from the Forensic Computing Unit as well as read only access to the FCU manager and 2 NHS Protect internal auditors, whilst approximately 30 staff from the National Investigations Service have access to the portal that links directly to the system.

11	For each organisation, what personal data is shared and for what purpose?	Access to the Lima Forensic Case Management System is restricted to five members of staff from the Forensic Computing Unit as well as read only access to the FCU manager and 2 NHS Protect internal auditors, This access is required to understand the subject, to conduct key word searches and undertake the forensic investigation. Approximately 30 staff from the National Investigations Service have access to the portal that links directly to the system; however they have restricted access to their own specific requests and subsequent forensic investigations only.
12	Is personal data shared with external organisations? (If No go to Q15)	Once in Lima, the data will only be disclosed if requested from CPS.
13	Is personal data shared with external organisations that are not within the [2]European Economic Area?	N/A
14	For each external organisation, what personal data is shared and for what purpose?	Once in Lima, the data will only be disclosed if requested from CPS. This would be for the administration of justice as the results would be used as evidence to assist in proceedings relating to an offence.
15	How is the personal data transmitted or disclosed to internal and external organisations?	Disclosure from Lima would only happen on request from CPS and for a specific investigation. This is not common practice and happens very rarely. In such instances the lima case record can be exported and would be given to the OIC/disclosure officer (Officer in charge) who would then make their own arrangements to supply this to CPS.
16	How is the shared personal data secured by the recipient?	It would be the responsibility of the recipient - eg an OIC or CPS to keep the data safe.

[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?	Access to the Lima Forensic Case Management System is restricted to five members of staff from the Forensic Computing Unit as well as read only access to the FCU manager and 2 NHS Protect internal auditors, This access is required to understand the subject, to conduct key word searches and undertake the forensic investigation. Approximately 30 staff from the National Investigations Service have access to the portal that links directly to the system; however they have restricted access to their own specific requests and subsequent forensic investigations only.
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?	Access to the Lima Forensic Case Management System is restricted to five members of staff from the Forensic Computing Unit as well as read only access to the FCU manager and 2 NHS Protect internal auditors, This access is required to understand the subject, to conduct key word searches and undertake the forensic investigation. Approximately 30 staff from the National Investigations Service have access to the portal that links directly to the system; however they have restricted access to their own specific requests and subsequent forensic investigations only.
21	What is the current accreditation of the system?	Official (Sensitive)

Table 2 - PIA Screening Questionnaire

5. 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 complete.

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

Table 3 – PIA Decision Criteria

[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.

Screening Process Conclusions

6. The screening process, completed in October 2017, identified the following PIA requirements of using the Lima Portal and Forensic Case Management System.

a. Although not undertaken at the beginning of the project, 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 https://ico.org.uk/media/for-organisations/documents/1042836/pia-code-of-practice-editable-annexes.docx

c. The following legal requirements apply to the system and in addition to this there is also a Risk Assessment report available.

i. Data Protection Act 1998

ii. Human Rights Act 1998

iii. Freedom of Information Act 2000

7. 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 Lima Portal and Forensic Case Management 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: PIA Report

Data Collection and Maintenance

1. The Lima Portal and Forensic Case Management System holds personal data and information in relation to forensic investigations. This includes contemporaneous notes as well as acquisition and analysis information. It also stores requests from officers in charge of the case as an automatic transfer from the Lima Portal.

a. The following personal data could potentially all be included:

Name, address & contact details, date of birth. Nationality, NI number & Passport Number. NHS Number, Driving Licence Number, Payroll Number of Subject. Professional Body Subject registered to. Professional Registration Number NHS Employment / links to NHS Details of NHS Department to where subject may be attending for treatment. Detailed description. Bank details. Details of credit history and personal checks, Vehicle details. 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 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. The impact level of the Lima Portal and Forensic Case Management System was assessed as CONFIDENTIAL and can only be accessed by a restricted number of staff from the Forensic Computing Unit and National Investigations Service.

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

a. Access to the Data Centre containing the Lima software is behind a combination lock door system.

b. 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.

c. Audit Logs exist if required.

d. All Forensic IT infrastructure is stored in locked cabinets.

e. All security incidents logged with the Information Security Manager and Information Security Officer.

f. The Lima Portal has a direct interconnection to the Lima Forensic Case Management System but not with any other NHS Protect systems and applications.

g. 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 NHSProtect register and the NHS Protect DPO is aware of its existence.

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

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

6. The privacy risks and associated mitigations are described in Table 4. The IAO is responsible for mitigating the risk.

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.	The data is collected in order for a forensic investigation to be conducted. It wouldn't be used for any other purpose.
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.
3. There is a risk that personal data is retained for longer than necessary.	The Lima Portal and Forensic Case Management System are subject to NHS Protect Data Handling and Storage Policy and will be 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.	As the information has been provided by Local Counter Fraud Specialists / other external government investigators or Senior Fraud Investigators from NHS Protect it would be checked by the lead investigator during the evidence gathering phase of the fraud investigation prior to being added to the Lima Portal and subsequently transferred to the Case Management System. NHS Protect has no means to audit or review this data for accuracy.
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 have been identified and 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 an external organisation.
8. There is a risk that personal data is hosted or exported outside of the EU.	No data will be exported outside the UK

Table 4 – Privacy Risks

Section 2: Uses of the Application and the Data

7. The Lima Forensic Case Management System is a system used by NHS Protect Forensic Computing Unit to store and manage all requests for Forensic Investigations to be conducted in respect of allegations of fraud, bribery and corruption within the NHS. Requests are received either as an automatic transfer from the Lima Portal when the internal Senior Fraud Investigator adds the request as a case log, or on receipt of a completed request for work form from external Local Counter Fraud Specialists (LCFS) in Scotland, Counter Fraud Wales, the police force, HMRC and DH. The Lima Forensic Case Management System contains all information in relation to each forensic investigation, contemporaneous notes as well as acquisition and analysis information in relation to the work carried out. It also stores the requests from officers in charge of the case and has the option to allow the notes to be linked back to the Portal so that the respective officer can view.

8. The data is collated collectively in a Case Management System and as individual cases in a Portal as well as in external request for work forms.

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

    a. Access to the Lima Forensic Case Management System is restricted to five members of staff from the Forensic Computing Unit as well as read only access to the FCU manager and 2 NHS Protect internal auditors, whilst approximately 30 staff from the National Investigations Service have individual area access to the portal that links directly to the system.

    b. The Lima Forensic Case Management System has a direct interconnection with the Portal and information in the Portal has originated from (FIRST) Fraud Information Reporting System Toolkit.

    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

10. Data will be retained only as long as necessary, up to a maximum period in accordance with the Data Protection Act 1998. The retention period for Lima is 7 years where fraud is found and 15 months where not. The data will be stored in digital format and will be erased, from the relevant storage server when no longer required. The IAO is required to review the retention period and any requirement to change must be submitted to the Application Change Board.

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

Section 4: Internal Sharing and Disclosure of Data

12. Data is not shared or disclosed other than as indicated in 9a above.

Section 5: External Sharing and Disclosure of Data

13. Once in Lima, the data will only be disclosed if requested from CPS. This would be for the administration of justice as the results would be used as evidence to assist in proceedings relating to an offence.

Section 6: Notice/Signage

14. It would be inappropriate for NHS Protect 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.
15. 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.
16. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this system or the counter fraud project behind it and is therefore outside the scope of this PIA.

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

17. 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.
18. It is unlikely that many access requests will be received as the personal data recorded is all in relation to fraud investigations that are confidential until such point they are substantiated
19. In the unlikely event that that information in relation to the subject is identified as being incorrect the record would be updated.
20. 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

21. The security and technical access architecture of the Lima Portal and Forensic Case management System is as explained in this PIA:

    The application and the hosting infrastructure was assessed at Official Sensitive and the hosting infrastructure is subject to CESG approved IT Security Health Check.
22. Access is restricted to staff in the Forensic Computing Unit and National Investigation Service using roles to assign specific privileges to both the Portal and the Case Management System.
23. 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

24. The Lima Forensic Case Management Software from IntaForensics used by NHS Protect, comprises of a Portal and Forensic Case Management system and is located in the NHS Protect/NHS Counter Fraud Authority data centre – although logical access is restricted to FCU staff and the Information Security & Systems Lead / Security and Operational Support Specialists only.

Conclusion

25. There are no residual privacy risks to the personal data recorded in the system. The controls described in this PIA explain 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 4: Compliance Checks

DPA 98 Compliance Check

1. The DPO must ensure that the Lima Portal and Forensic Case Management System, 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 NHSProtect 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 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 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 – Lima Portal and Forensic Case Management System Personal Data

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

No	Personal Data	Justification
1	Name, address & contact details, date of birth. Nationality, NI number & Passport Number. NHS Number, Driving Licence Number Payroll Number of Subject. Professional Body Subject registered to. Professional Registration Number NHS Employment / links to NHS Details of NHS Department to where subject may be attending for treatment. Detailed description. Bank details. Details of credit history and personal checks Vehicle details. 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 ***Sensitive Data as listed in Annex A of PIA*** **Commission or alleged commission of offences for Subjects.* **Proceedings relating to an actual or alleged offence for Subjects*. **Racial or ethnic origin of Subject*	The data is required to understand the subject of the investigation. The data would not be used for any other purpose.

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	Lima

2. Contact position and/or name
(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

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 Lima Portal and Forensic Case Management System is a system used by NHS Protect to store and manage all requests for Forensic Investigations to be conducted in respect of allegations of fraud, bribery and corruption within the NHS. Requests are received either as an automatic transfer from the Lima Portal when the internal Senior Fraud Investigator adds the request as a case log, or on receipt of a completed request for work submission form from external Local Counter Fraud Specialists (LCFS) which also includes Scotland, Counter Fraud Wales, the police force, HMRC and DH.

The system contains all information in relation to each forensic investigation, contemporaneous notes as well as acquisition and analysis information in relation to the work carried out. It also stores the requests from officers in charge of the case and has the option to allow the notes to be linked back to the portal so that the respective officer can view. Email notifications are received when a case log is updated.

The investigation would involve seizing a computer or forensic acquisitions on site under a warrant. The most common request is for a key word search or emails between certain dates. The notes of the results would be added to the system where they can be viewed by staff in the Forensic Computing Unit and National Investigation Service dependant on specific permissions to the system.

The results would then be used as evidence to assist in proceedings relating to an offence.

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.

The purpose of the Lima Portal and Forensic Case Management System is to manage requests for forensic investigations in order to provide evidence to assist with the outcome of an investigation in respect of allegations of fraud bribery and corruption within the NHS.

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

Privacy impact assessments have been considered in the light of personal data gathered, and the data in Lima 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 4 of this document)

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

This is the first PIA 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.

(Data Protection Act, section 1)

NHS Protect offices

Coventry

Cheylesmore House
5 Quinton Road
Coventry
West Midlands
CV1 2WT

London

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

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH