NHS
Counter Fraud Authority

CLUE Case Management and Intelligence System

Data Protection Impact Assessment

May 2021

V3.0 Published Version

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

Executive Summary

This document contains information in relation to the CLUE Implementation (FIRST replacement) Project.

CLUE3 has been purchased to replace the existing NHSCFA Fraud Investigation Reporting System (FIRST) case management system.

CLUE3 is a UK cloud based product that will contain the existing investigation and intelligence data, as currently held in FIRST. CLUE3 has additional capability such as the management of raw intelligence information and recording confidential sources. The use of this capability is under consideration but implementation would not be expected until 2021/22 or later. As a cloud based system, this is a third party hosted product to allow 24hr web-based access.

The nature of a cloud based system requires the third party provider, CLUE, to manage the data security of information.

The data security requirements of CLUE, as the third party provider of the CLUE3 system, are set out in the project contract (agreed 23rd March 2018) and associated addendum policies as listed below:

Azure-Cyber Essentials PLUS Certificate 2020
Azure-UK G-Cloud Security Assessment (May 2019)
CLUE-Cyber Essentials 2020/21
Clue ISMS Overview Document
ISO 27001

The information contained within this document is categorised OFFICAL.

Any information viewed/obtained within this document 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'**

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

Table of Contents

Document Control					
Completed By	**Ref**	**Document owner**	**Version**	**Issue Date**	**Amendments**
Clue Implementation Lead	DPIA CLUE	DPO	V0.1	October 2019	Initial Draft
Clue Implementation Lead	DPIA CLUE	DPO	V0.2	November 2019	Amendments to initial draft
Clue Implementation Lead	DPIA CLUE	DPO	V1.0	December 2019	Final Version
Clue Implementation Lead	DPIA CLUE	DPO	V1.1	December 2020	Annual Update
Clue Implementation Lead	DPIA CLUE	DPO	V2.0	December 2020	Amendments
Clue Implementation Lead	DPIA CLUE	DPO	V2.2	January 2021	Final version following review and amendments
Clue Implementation Lead	DPIA CLUE	DPO	V3.0	May 2021	Further redaction for external publication

Prefix	
Reference:	DPIA CLUE
Date:	May 2021
Author:	Clue Implementation Lead
Data Owner:	Head of Operations
Version:	3.0
Supersedes	2.2

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	May 2018	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
Organisational Strategy	Leading the fight against NHS fraud	All	2017	NHSCFA
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

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:

"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.

CLUE General Description

10. CLUE is a single web based application used to manage investigations of fraud including referral, incident, risk, intelligence, investigation, case and outcome management. CLUE will be used to support the NHSCFA organisational strategy objective of being the single expert intelligence led organisation providing a centralised investigation capacity for complex economic crime matters in the NHS.

11. For security and confidentiality purposes, the database is accessed by approximately:

- 100 members of staff from NHSCFA, which includes the database administrators
- 6 members of staff from the Department of Health and Social Care
- 25 members of staff from the NHS Counter Fraud Service Wales and Local Counter Fraud Specialists based in Wales.
- 209 Local Counter Fraud Specialists employed by, or provide a service, to NHS organisations and those providing services to the NHS.

12. Authorisation and access for Local Counter Fraud Specialists is managed through the NHSCFA LCFS nominations process which requires a LCFS to hold Accredited Counter Fraud Specialist certification. This is managed by the NHSCFA Organisation Development Directorate. NHSCFA staff will be added by the service desk or the implementation project and will be managed through the existing new starter and leaver processes.

13. This is the o*nly* DPIA to be completed on the CLUE system and it has been carried out by the Information and Records Management Officer, in consultation with the Clue Implementation Lead, and the data owner, (Head of Operations)

14. CLUE, 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

15. To ensure that CLUE 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 fully functional and flexible case management and intelligence system with capabilities including: subject, witness and 'other' contact recording; subject checks, accounts, assets, examinations and criminality; key date recording, including results and disposals. Able to support the generation of all template based documentation, e.g. Schedules, Prosecution Case Files, MG Forms and advice files. For investigators, CLUE will have the capability to support information exchange with the CPS by exporting case files and exhibits to their systems and also be able to import forensic software toolkits. This will assist the investigations team in managing information and reducing transposition errors. This capability is not currently available to the NHSCFA but will be revisited in the near future. CLUE will interact with the NHSCFA intelligence database via Microsoft Power Query. Inclusion of this database in the intelligence data will allow for information to be processed and searched by intelligence officers and analysts. This will allow the NHSCFA to identify trends in crime and ensuring new information to ongoing investigations is disseminated as a priority. CLUE provides Local Counter Fraud Specialists the ability to report intelligence securely to the NHSCFA. This personal information will be used to prevent crime against the NHS and users of this database are managed by the Central Intelligence Team's Senior Intelligence Database Officer. Personal information will be downloaded through CLUE's Application Programming Interface and imported into the NHSCFA's existing analytics system (SAS). This is to allow for reporting on information suitable to answer Freedom of Information (FOI) and Parliamentary Questions (PQ) requests' and also allow for the extraction of management reports. The content of the management reports will **not** contain personal information. CLUE contains special category information of personal data which the data subject may not be aware the NHSCFA are processing. 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.

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. Data will be collected by investigation and intelligence staff from across the wider health group. For intelligence staff, how this data is collected is already subject to DPIAs including those for the Fraud and Corruption Reporting Online (FCROL) and the NHSCFA Intelligence Database. For investigations staff this information will be collected in accordance with the NHSCFA's Fraud Manual. Data retention periods are followed as agreed in the NHSCFA data retention schedule.

2. The source of the information can vary but includes and is not limited to members of the public, members of NHS staff and the Department of Health and Social Care, other law enforcement agencies and regulatory bodies. Other sources of information include those which are openly accessible such as news and social media websites.

3. The NHSCFA may be required to share this information with other organisations. This may be to support another organisation in carrying out their statutory duty in which case this information will be shared under a memorandum of understanding or other legal gateway. These organisations may include the police, law enforcement agencies, regulatory bodies and NHS organisations or organisations providing a service to the NHS. Information shared with the CPS will be completed using EGRESS although an automated function is built within CLUE; all other information shall be shared on a case by case basis using built in tools within CLUE.

4. The information contained within CLUE could be used for data matching, will involve invisible processing and risk of physical harm. This data will also include data consisting of the commission or alleged commission by him of any offence; or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. All of which are considered examples as likely high risk processing.

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 obtained by the NHSCFA is in line with those required for the prevention and detection of crime. This will uniquely identify a person which will require information such as the person's name, date of birth, any unique identifiers such as National Insurance and Driving Licence numbers, linked addresses, occupation and work history, financial history and descriptions. Due to the nature of the role of the NHSCFA, special data categories may need to be collected around the health, ethnic origin, race, and biometric. As an organisation it is possible that information that will be captured as part or arrests and searches that meet the other special categories. CLUE will also hold Police National Computer disclosure prints which will show criminal offence data for subjects and the system will also be used to record successful prosecutions of fraudsters.

2. At present there are less than 1,000 persons recorded on CLUE and expected to increase by 6,000 per year from 2021/22. This number may then reduce from mid 2022/23 when the CLUE retention policy will require deletions to be made from the case management system.

3. Information will be collected daily, mostly between Monday-Friday but weekend working cannot be ruled out

4. Information is retained in accordance with the NHSCFA Operations Retention Schedule. Retention and deletion processes can be found in Part 2.

5. See point 2 above.

Mostly England and Wales, although DHSC does have a remit for the United Kingdom. The NHSCFA also receives reports about subjects defrauding the NHS from overseas so information may be held on persons living abroad.

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. Data subjects fall into 5 main categories
    a. Source: Someone who has reported information to prevent financial crime within the NHS. This may be a whistle-blower, a staff member who has a responsibility to report fraud, a member of the public, or an external organisation such as a regulatory body or law enforcement agency.
    b. Subject and Persons of Interest: Persons who are associated with a possible crime against the NHSand may be investigated.
    c. Witness: A person who has provided information to support or disprove an allegation of fraud against the NHS.
    d. Staff: Information about staff using CLUE may be collected throughout an investigation, however this is most likely to be business information such as email addresses. It is possible, however, that personal information such as date of birth may be required for witness statements or that a staff member has a previous conviction may be required for an MG9 witness list.
    e. Patients: The NHSCFA may be required to collect information on patients to prove there is a fraud.

2. As the information will be required for the prevention and detection of crime, or another legislative purpose, there are exemptions which will mean the rights of the data subject are limited. For sources they can minimise their data by being an anonymous, confidential (limiting who has access to their data) and named where they consent to their details being linked to a report. For subjects and persons of interest they are unlikely to be aware that we are processing their data until they are interviewed under caution or arrested and as such will not have control of their data.

3. For subjects and persons of interest, they may not expect their data to be being processed. This is because they have not provided the information and the nature of the data could prejudice an investigation or result in harm to a source limiting the rights of the data subject. The NHSCFA offer a number of options for sources of information to provide their information and can chose to withhold their information. For witnesses and staff they would expect their data to be processed by the NHSCFA in this way. Information on other persons is collected as evidence including those on patients to prove a fraud. This information will be collected under exemptions include in the Data Protection Act 2018 or powers afforded in the Health Act and the collection of this information is made on a case by case basis as to whether the data subject needs to be informed.

4. Due to the nature of the work of the NHS it is possible that witnesses could include children and persons from other vulnerable groups.

5. There are no prior concerns or known security flaws regarding this type of processing, which is not novel for the industry. Technology in this area has evolved, with greater use being made of cloud-based solutions. As CLUE will be hosted on the Microsoft Azure cloud platform, a range of security measures will be in place to protect the system and data from unauthorised access. More details are available on the entry for Clue Computing Company on the government's Digital Marketplace at https://www.digitalmarketplace.service.gov.uk/g-cloud/services/393981736680662 (CLUE has been approved as a service public sector bodies can procure under a framework agreement). There is an export function within CLUE, however users can only export the information that they have permission to access.

6. No. Recording this information on a case management and intelligence system is standard practice and was previously carried out by the NHSCFA on the previous case management system.

7. Covered in paragraph 5 above. Technology in this area has evolved, with greater use being made of cloud-based solutions. As CLUE will be hosted on the Microsoft Azure cloud platform, a range of security measures will be in place to protect the system and data from unauthorised access

8. No issues of public concern should be highlighted. As with all internal NHSCFA communications, the information will be handled in accordance with the terms and conditions of use as well as policies regarding acceptable use, standards of business conduct and policies and procedures relating to information sharing.

9. Both the NHSCFA Clue have an 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 provide a case management and intelligence sharing system to prevent, identify, record and recover NHS monies lost to fraud, bribery corruption.

2. For subjects or persons of interest of an investigation the intended effect is to establish if they have committed a crime or not. For other data subjects it is to ensure that their information is recorded accurately and securely to support enquiries.

3. To prevent, identify and recover NHS monies lost to fraud, bribery and corruption.

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. The NSHCFA has approached teams within the NHSCFA as well as the wider counter fraud community as to what requirements they have for a case management system. This took place as part of the procurement exercise of CLUE. Throughout the implementation of CLUE all teams have been consulted to identify issues and opportunities for the system.

2. There is an ongoing requirement to liaise with NHSCFA teams and wider health group LCFSs.

3. Clue, the company, will need to assist with the migration from the current NHSCFA Case Management System – FIRST. They will also be required for any bulk importing into CLUE. Clue may also be required for other ad-hoc work such as the initial creation of user accounts and bulk updating of records.

4. The NHSCFA Information Security and Systems Lead has been consulted.

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. Public Task -Prevention and Detection of crime in the NHS.

2. Yes

3. In theory it could be done with pen and paper but this would be impractical.

4. The NHSCFA receive training throughout the year on the Data Protection Act 2018 and the use of data for its collected purpose. We will prevent function creep by keeping our processing under periodic review – we do not expect the purpose of processing to change following release of the system.

5. Checking of information in an investigation is problematic due to the free text nature of the information collected ruling out validation and automated checking on the majority of fields. Fields on CLUE are limited where possible to set values to prevent typing errors. Investigations are reviewed by IMOs and investigation leads and the information is accessed by multiple applications and users which should flag inaccuracies. Reports can be run on the SAS system to identify information that may be incorrect such as subjects born in the future or are under 16. Retention reviews will be undertaken to limit the time the information is held for. Information collected for the purposes of the prevention and detection of crime will have to be considered for necessity and proportionality. However, due to requirements under CPIA 1996, it may be necessary to retain information which may not be relevant.

6. Individuals can make requests to the NHSCFA by a subject access request. This is considered by the Information Governance team and a decision is made on what information to release. Due to the type of processing, a subject's rights may be limited. How we handle personal data, our legal basis for processing and who we work with and may share data with is outline in our website's privacy policy.

7. As with No.6 above the website explains the rights of data subjects subject to relevant exemptions and the process to be followed.

8. We will periodically seek assurance from the suppliers of their continued compliance with applicable data protection rules, and we will work with the information security and information governance team to flag up and address any concerns. Schedule 7 and 14 of the CLUE/NHSCFA contract stipulate the requirements of the suppliers.

9. To progress an investigation, it may be necessary for enquiries to be made with organisations outside of the EEA. This would usually require sharing the name and date of birth of a subject although other information may need to be shared such as passport numbers. This is an investigations process though rather than a use of CLUE.

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
1. There is a risk that the personal data is used for other purposes than for what it was originally intended for.	Possible	Significant	Low
2. There is a risk that personal data is retained for longer than necessary	Possible	Minimal	Low
3. There is a risk that the personal data is no longer relevant.	Remote	Minimal	Low
4. There is a risk that the personal data is not accurate or up to date.	Remote	Minimal	Low
5. There is a risk that the confidentiality of the personal data is not adequately protected.	Possible	Minimal	Low
6. There is a risk that personal data is passed to external organisations.	Possible	Significant	Low
7. There is a risk that personal data is passed to external organisations.	Possible	Significant	Low
8. There is a risk that personal data is hosted or exported outside of the EU.	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
a. Users are only given sufficient rights to systems to enable them to perform their specific job function. User rights will be kept to the minimum required to do their job effectively and efficiently. Access rights are reviewed on a monthly basis and controls are placed on how much information can be exported to be used for other purposes.	Reduced	Low	
b. This DPIA exists to ensure that there is due consideration as to the extent of the data used. Investigators and intelligence officers also have to consider the proportionality and justification for all information that they look to collect the information initially. Information is also reviewed by the Information Management Officers and NIS managers so that any issues can be highlighted to investigations and intelligence staff to avoid any future issues.	Reduced	Low	
c. CLUE is subject to NHSCFA Data Handling and Storage Policy and is audited annually to ensure that personal data is not retained longer than necessary.	Reduced	Low	
d. 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. There are also legislative reasons such as CPIA 1996 that requires the NHSCFA to retain this data for a set period and the Police Management of Information sets out the principles for processing information for a policing purpose.	Reduced	Low	
e. CLUE data is provided by various sources and updated as the investigation progresses. As such, the responsibility for accuracy lies with the responsible officer for the report. Where possible checks are made to corroborate information. The application interfaces within CLUE can be used to identify obvious mistakes such as transposition errors when entering data manually into CLUE.	Accepted	Low	

f. CLUE is protected by a multifactor authentication protected system which requires a username, a password and a device known to the user. Permissions are allocated to staff on a role and organisation basis so that they only see personal information which is required for their role.	Reduced	Low	
g. Requests by other agencies need to be made in writing to the NHSCFA. Officers determine whether the request is proportional or necessary before releasing the information. It may be necessary to release information to external agencies such as other law enforcement agencies for crime and regulators to conduct functions designed to protect the public.	Accept	Low	
h. It is possible that data may be exported outside of the EU but this would be on a case by case basis and decided by the NHSCFA Information Governance team.	Accept	Low	

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: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the new system has been undertaken. Access to the system will be strictly controlled by IT administrators and it will be protected by a multifactor authentication process which requires a unique username, a passwords and device known to user being assigned to an LCFS. LCFSAs will only have access to their own Trust case materials, thereby making its use fully auditable. While the system will hold personal, special category, criminal convictions and offence data there are appropriate organisational measure in place to ensure that it is held safely and securely and all such data will be held in accordance with current data protection legislative requirements and organisational best practice and it's data retention policy. I am therefore satisfied with the organisational security measures employed.		
Consultation responses reviewed by:	Trevor Duplessis 28th January 2021	If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Ownership

16. The following table describes the CLUE roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Head of Operations
Senior Responsible Officer (SRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Head of Operations
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. The system will be the sole Case Management System for NHSCFA

2. It will contain data to be used for the prevention and detection of crime. (or see General description (page 10)

3. The impact level of CLUE was assessed as OFFICIAL SENSITIVE and it can only be accessed by staff within the NHSCFA and those in the wider counter fraud group including DHSC AFU, Counter Fraud Service Wales and LCFSs.

4. The following measures briefly describe what controls have been implemented to protect CLUE and the personal data recorded:
    a. CLUE is a 'software as a service' (SaaS) solution, hosted in an external data centre and as such the NHSCFA has no control over security measures in place. However, the credentials, certifications and assertions of both the hosting data centre (Microsoft Azure) and of the software supplier (CLUE) can be checked.
    b. CLUE is only accessed by approximately 340 members of staff from across the wider healthcare community, which includes the database administrators
    c. CLUE does have the ability to link with other NHSCFA systems such as SAS. Further connections may be made in the future to automate administrative routines such as linking to directories to ensure user access data is accurate.
    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.

5. It is assessed that there are no residual privacy risks to the personal data used by the use of CLUE.

6. 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

7. CLUE holds details of investigations relating to fraud, bribery and corruption within the NHS The information is collected for the identification and analysis of suspects involved in acts of fraud bribery and corruption within the NHS.

8. CLUE is administered by the CLUE implementation Leads.

9. Information in CLUE could include:
    a. **For the source**: name, address and contact details. Please note that a source may also be a witness or a subject.
    b. **For CLUE users**: Name and business address and contact details. Please note that a CLUE user could also be a witness.
    c. **For the subject**: Name, address, date of birth, contact details, nationality, NI number, passport number, racial or ethnic origin, NHS number, driving licence number, payroll number, details of professional body including registration number and sanctions, NHS employment details or any links to NHS including department where treatment is being received, details of any other occupation/employment, full description including height, hair style, length and colour, whether any facial hair, eye colour, body type, and if there are any distinguishing features marks or scars. Bank Details including name, address and phone number, sort code and account number, Vehicle Details including make, model, colour, age and licence registration plate. Details of any commission or alleged commission of offences, Proceedings and outcomes relating to an actual or alleged offence, Details of credit history and other personal checks including links to UK companies and data held by other law enforcement agencies. Information collected through use of legislation available to the NHSCFA including information linked to surveillance, communications data and the Health Act.
    d. **For the witness**: name, address, date of birth, contact details, employment information and previous criminal convictions.

10. Special category data included in CLUE can include:
    a. race;
    b. ethnic origin;
    c. politics;
    d. religion;
    e. trade union membership;
    f. biometric data;
    g. health;
    h. sex life; or
    i. sexual orientation.

11. The measures that have been implemented to protect the Personal Data are:
    a. Access is restricted to approximately 100 members of staff within NHSCFA including the database administrators.

    b. CLUE has a direct interconnection with SAS through the CLUE Application Programming Interface which is accessed through an API username and key. SAS has a built in feature which allows the system to collect information from a web service and natively import the data into SAS.

    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. CLUE is subject to NHSCFA Data Handling and Storage Policy. Paper records are held by the both the Information and Intelligence Unit and the National Investigation Service. Local Counter Fraud Specialists are responsible for hard copy information.

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. Access is restricted to approximately 100 members of staff within NHSCFA including the database administrators.

Section 5: External Sharing and Disclosure of Data

15. Information may be shared with other organisations such as the Police, other law enforcement agencies, regulatory bodies and Local Counter Fraud Specialists in accordance with NHCFA legal gateways.

Section 6: Notice/Signage

16. The data subject may not be informed that we hold information on them if it would prejudice law enforcement or the rights and freedoms of another person.

17. 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.

18. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to CLUE 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 all in relation to an offence which may result in an investigation, and as such are confidential until such point they are substantiated.

20. In the 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 CLUE 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. Access is restricted to those investigation, analysing and preventing economic crime in the NHS in England, Wales and the Department of Health and Social Care.

24. The technical controls to protect the database are as described above in Section 1: Overview of Data Collection and Maintenance 4(a)

Section 9: Technology

25. CLUE holds personal information taken both by telephone and electronically and is located in a Microsoft Azure cloud computing platform.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that CLUE, 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. CLUE will be hosted on the Microsoft Azure cloud platform, and as such, a range of security measures will be in place to protect the system and data from unauthorised access. More details are available on the entry for Clue Computing Company on the government's Digital Marketplace at **https://www.digitalmarketplace.service.gov.uk/g-cloud/services/393981736680662** (CLUE has been approved as a service public sector bodies can procure under a framework agreement).

4. CLUE 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 A Section 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 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 CLUE. 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 OPERATIONS
Project	CLUE Implementation

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.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.

CLUE is a single web based application used to manage investigations including referral, incident, risk, intelligence, investigation, case and outcome management.

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

NHSCFA leads on a wide range of work to protect the NHS from economic crime. CLUE will be used to support the NHSCFA organisational strategy objective of being the single expert intelligence led organisation providing a centralised investigation capacity for complex economic crime matters in the NHS Access is restricted to 100 members of staff within NHSCFA, including the database administrators.

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

Dare Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in CLUE 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).

DPIA-CLUE Case Management and Intelligence System V1.0.

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	London	Newcastle
9th Floor	4th Floor	1st Floor
Earlsdon Park	Skipton House	Citygate
55 Butts Road	80 London Road	Gallowgate
Coventry	London	Newcastle upon Tyne
CV1 3BH	SE1 6LH	NE1 4WH