Counter Fraud Authority

NHSCFA Complaints Process

Data Protection Impact Assessment

September 2023

V2.0 Published

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

Executive Summary

This document contains information in relation to NHSCFA Complaints Process

The document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (June 2023).

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

Government Security Classifications Policy June 2023.docx (publishing.service.gov.uk)

In particular please note that:

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

Table of contents

Executive Summary **2**

Links & Dependencies **5**

1. Data Protection Impact Assessment Requirement & Process **6**

Introduction 6

System Name - General Description 7

Data Protection Impact Assessment 7

Ownership 18

2. DPIA Report **18**

Section 1: Data Maintenance and Protection Overview 18

Section 2: Uses of the Application and the Data 18

Section 3: Data Retention 19

Section 4: Internal Sharing and Disclosure of Data 19

Section 5: External Sharing and Disclosure of Data 19

Section 6: Notice/Signage 19

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

Section 8: Technical Access and Security 20

Section 9: Technology 20

3. Compliance Checks **20**

DPA 2018 Compliance Check 20

The Privacy and Electronic Communications Regulations 20

The Human Rights Act 21

The Freedom of Information Act 21

Conclusion 21

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

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

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Counter Fraud Specialist & Complaints Investigator	Complaints Process	DPO	V1.1 Draft	27/07/2023	Revised from previous version of template
Counter Fraud Specialist & Complaints Investigator	Complaints Process	DPO	V2.0 Draft	22/08/2023	Updated for publication
Counter Fraud Specialist & Complaints Investigator	Complaints Process	DPO	V2.0	22/09/2023	Published

Prefix	
Reference:	DPIA NHSCFA Complaints Process
Date:	27/07/2023
Author:	Counter Fraud Specialist & Complaints Investigator
Data Owner:	Corporate Affairs Manager & Board Secretary
Version:	2.0
Supersedes	V1.1 Revised from NHS PROTECT PIA - Complaints Process

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	June 2023	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

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

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

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

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

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

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

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

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

    a. use new technologies;

    b. match data or combine datasets from different sources;

    c. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

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

[1] GDPR - Recital 75

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 Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

NHSCFA Complaints Process - General Description

10. The NHSCFA Complaints Process is a mechanism to provide the opportunity to the public to raise any expression of dissatisfaction that requires a response. Two individuals have access to the information which is held in restricted folders.

11. The data is collected voluntarily from the complainant or their representative in the form of an electronic online form, email, letter or phone call, and saved in restricted folders.

12. This is the first DPIA to be completed on the Complaints Process, and supersedes the original PIA completed for NHS Protect. It has been completed by the Information and Records Management Officer, in consultation with Counter Fraud Specialist & Complaints Investigator and the Information Governance and Risk Management Lead.

13. The Complaints Process 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

14. To ensure the Complaints Process 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.

The purpose of a NHSCFA Complaints process is to provide the opportunity to the public to raise any expression of dissatisfaction that requires a response. For example, claims of unfair treatment by the NHSCFA, dissatisfaction about how the NHSCFA has dealt with a situation, claims that a poor standard of service has been provided and claims that NHSCFA staff have been unhelpful or rude.

As part of the complaint handling process individual's personal/sensitive data will usually be processed and is provided voluntarily by the complainant. Data collected is usually name, address, email address, date of birth, contact details and where appropriate details of employment and occupation. It may also include details of physical or mental health or condition, commission or alleged commission of offences; or proceedings relating to an actual or alleged offence where it is deemed relevant to provide by the complainant.

The NHSCFA Complaints process comprises of an electronic log of informal and formal complaints consisting of an Excel spreadsheet held in a restricted access area, with the corresponding material stored in a restricted Teams folder. Additionally there is an Outlook folder, again with restricted access, for email communication in which online reporting forms are also received.

The NHSCFA Complaints Process, is required to comply with relevant HMG legislation including where applicable the Data Protection Act 2018 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 DPIA which is broken down into the following stages:

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

b. DPIA Assessment and Report;

c. Compliance Checks;

d. Summary and Conclusions

STEP 2: Describe the processing

Describe the nature of the processing:

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

2. What is the source of the data?

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

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

1 The data is collected voluntarily from the complainant or their representative in the form of an electronic online form, email, letter or phone call. Information is stored in restricted folders and deleted in line with the Data Retention Schedule

2 Members of the public will voluntarily share personal information as part of their complaint.

3 Data may be shared internally at stage 1 with the Government & Assurance Lead (GAL) for oversight and the Central Intelligence Team (CIT) to help establish whether there is any operational history that may affect the ability to take the complaint forward. The information may also be shared with the Head of Operations & Engagement (HO&E), as decision maker to decide whether a complaint should be progressed/deferred where complaints relate to investigations and there is an active investigation. The information is also shared at final sign off with the CEO. Where a complaint has been escalated to a stage 2 complaint the information will be shared with the Board Chair (or other Board member) as they are responsible for producing an independent response in these instances. Data may be shared externally where there is a stage 3 complaint escalation at the request of the Parliamentary Health Service Ombudsmen (PHSO) to assist them in responding to their complaint.

4 N/A

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. Data collected is usually name, address, email address, date of birth, contact details and where appropriate details of employment and occupation. It may also include details of physical or mental health or condition, Commission or alleged commission of offences; or proceedings relating to an actual or alleged offence.

2. As above

3.As and when received

4. The data will be kept for 7 years, as stipulated for complaints in the CFA Data Retention Schedule.

5. Only the complainants.

6. National – UK only.

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. Complainants are usually members of the public

2. Complainants have a measure of control, subject to any permitted exceptions. For example, a complainant may withdraw a complaint at any stage of the process and impose their 'right to be forgotten' which can be implemented where appropriate.

3. Information is provided voluntarily and where a standard acknowledgement is sent they are advised that personal information will be treated in compliance with all data protection legislation. Underpinning information on how their complaint is handled is also available in the CFA Complaints Policy.

4. The CFA Complaints Policy addresses the potential scenario in that complaints can be received by a representative on behalf of a child. Equally, vulnerable groups such as individuals with mental health issues may submit complaints. A representative may make a complaint on behalf of another person who is a child or has physical incapacity, or lack of mental capacity within the Mental Capacity Act 2005. We will not consider a complaint made by a representative until we are satisfied that there are reasonable grounds for the complaint being made by a representative. Where we are not satisfied that there are reasonable grounds for representation, the NHSCFA will notify in writing with the reason for the decision.

5. A Standard Operating Procedure for the management of complaints records has been created to follow to reduce the risk of processing errors or security flaws

6. No

7. Standard business software is used – Excel, Teams, Word, Outlook etc.

8. No

9. The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network.

Describe the purposes of the processing:

1. What do you intend to achieve?

2. What is the intended effect on individuals?

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

1.To facilitate a satisfactory response on behalf of the CFA to complaints raised by the public.

2.To resolve the complaint for the complainant, ensuring we are providing an effective, consistent, high standard complaints process to the public, providing them with the opportunity to resolve the matter(s) they have brought to the attention of the CFA.

3. Organisational benefits include compliance with Local Authority Social Services and National Health Service Complaints (England) Regulations (2009), adherence to best practice, ability to implement recommendations and improvements for the organisation resulting from any lessons learned, positive reputational impact etc.

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. Other than the restricted access provisions in place in terms of IT this would not be required.

2. Yes, CFA service desk were consulted to ensure restricted permissions in place for areas where complaints are held, such as Teams, Outlook and for online reporting.

3. As above. In addition an online complaint reporting form has been introduced which was implemented by IT.

4. As above

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?

2. Does the processing actually achieve your purpose?

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

4. How will you prevent function creep?

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

6. What information will you give individuals?

7. How will you help to support their rights?

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

9. How do you safeguard any international transfers?

1. Consent and public task

2. Yes it enables the resolution of their complaint.

3. No

4. Effective Standing Operating Procedures and Policies to outline roles and responsibilities within the process.

5. Complainants are encouraged to only provide information relevant to the complaint, for example the online form will ask questions to guide what details are required from them.

6. Only information related to their complaint is provided with restrictions in place where relating to any confidential information we may hold, for example updates on live operational activity.

7. The NHSCFA Complaints Policy provides transparency to the complainant in terms of their rights.

8. Standard Operating Procedure is in place to provide guidelines to administer an efficient processing in the handling of how information is dealt with.

9. N/A

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant, or Severe	**Overall risk** Low, Medium or High
Sharing of personal information resulting in reputational damage and negative impact on individual	Possible	Significant	Medium
External illegal access to information	Remote	Significant	Low
Misuse of data for purposes other than intended ones leading to privacy violations and loss of trust/reputational damage/damage to individual	Remote	Significant	Medium
Keeping personal data longer than necessary without a valid reason	Possible	Minimal	Medium

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 by SMT Owner Yes/No
Adherence to the Complaints Record Management Standard Procedure reduces risk of sharing personal information. Data minimisation to ensure only information that is required to process the complaint is provided, for example using the complaints reporting form guides as to what information is required.	Reduced	Low	Yes 7.8.23
Secure IT firewalls in place to reduce likelihood of external access to information illegally. Regular data back ups to reduce likelihood of data loss. In terms of internal unprohibited access, awareness and adherence to internal complaint record management standing operating procedure and IG training. Restricted permissions, granted only to those requiring access to relevant personal data, with regular reviews to ensure only appropriate individuals are able to view/access.	Reduced	Low	Yes 7.8.23
Awareness of Complaints Record Management Operating Procedure to avoid misuse of data for purposes other than intended ones leading to privacy violations and loss of trust/reputational damage/damage to individual. Second party oversight to ensure complaints information processor correctly handling information. IG training to raise awareness of correct protocols.	Reduced	Low	Yes 7.8.23
Data Retention Policy and Complaints Data Retention schedule adherence to ensure personal data is deleted where there is no valid reason to keep beyond the time period specified. Yearly reviews to ensure folders/emails only contain information within data retention schedule period.	Reduced	Low	Yes 7.8.23

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by SMT Owner:	Ann Sturgess 7.9.23.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by SMT Owner:	N/A	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 organisation's electronic Complaints Log has been carried out. The collation, use and storage of personal data is limited to only that required to achieve the required purpose with appropriate information made available to data subjects. The log is housed in a restricted access area, with corresponding material stored in a restricted Teams channel folder together with a restricted Outlook folder for email communication in which online reporting forms are also received. The Complaints Process log, associated Teams and Outlook channel and folder has restricted access to two members of staff. It is a standalone process that does not have any direct interconnections with other NHSCFA systems or applications. The limited based permissions are therefore fully auditable. All data will be held and governed in accordance with current legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the with the organisational security measures employed.		
Consultation responses reviewed by:	Trevor Duplessis - 22nd September 2023	If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by the Information and Records Management Officer:		The DPO should also review ongoing compliance with DPIA

Ownership

The following table describes the roles and responsibilities

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Corporate Affairs Manager & Board Secretary
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Counter Fraud Specialist & Complaints Investigator
Data Protection Officer	Trevor Duplessis

2. DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The impact level of the NHSCFA Complaints Process was assessed as OFFICIAL SENSITIVE and it can only be accessed internally.
2. The following measures briefly describe what controls have been implemented to protect the NHSCFA Complaints Process and the personal data recorded:
    a. The NHSCFA Complaints Process is accessed by approximately 2 members of staff from NHSCFA.
    b. The NHSCFA Complaints Process is independent, and does not have any direct interconnections with other NHSCFA systems and applications.
    c. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.
3. It is assessed that there are no residual privacy risks to the personal data used by the NHSCFA Complaints Process
4. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

5. The Counter Fraud Specialist & Complaints Investigator has responsibility for the administration of the NHSCFA Complaints Process

6. Information in the NHSCFA Complaints Process could include; name, address, email address, date of birth, contact details and where appropriate details of employment, occupation, physical or mental health or condition, Commission or alleged commission of offences; or proceedings relating to an actual or alleged offence.

7. Sensitive data may be processed including; physical or mental health or condition, Commission or alleged commission of offences; or proceedings relating to an actual or alleged offence.

8. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

9. The NHSCFA Complaints Process is subject to NHSCFA Data Handling and Storage Policy, and there is a manual deletion process after 7 years.

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

Section 4: Internal Sharing and Disclosure of Data

11. The NHSCFA Complaints Process is accessed by 2 members of staff from NHSCFA.

Section 5: External Sharing and Disclosure of Data

12. The only information shared with external organisations, would be if it was requested for the administration of justice.

Section 6: Notice/Signage

13. In most cases the data subject is made aware that we hold data for them, unless there is a serious allegation made against them - in which case they would be informed at the SMT's discretion.

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

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

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

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

16. It is unlikely that many access requests will be received as the personal data recorded is all in relation to complaints of which the data subject is already aware.

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

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

Section 8: Technical Access and Security

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

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

20. Access is restricted to internal staff only.

21. The technical controls to protect the NHSCFA Complaints Process include: Anti-virus protection;

a. Permission based access controls to shared drive.

b. Logging, audit and monitoring controls.

c. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

22. The NHSCFA Complaints Process holds personal information obtained electronically and is located in the NHS Counter Fraud Authority data centre.

3. Compliance Checks

DPA 2018 Compliance Check

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

   a. The GDPR and the Data Protection Act in general;

   b. The Data Protection Principles;

   c. The interpretations of the Principles.

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

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

4. The NHSCFA Complaints Process processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed (see Annex B) describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, See; also Annex A Category 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 the NHSCFA Complaints Process. 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	Corporate Affairs
Project	Complaints Process.

2. Contact position and/or name.
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

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

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

The NHSCFA Complaints process is a mechanism to provide the opportunity to the public to raise any expression of dissatisfaction that requires a response. For example, claims of unfair treatment by the NHSCFA, dissatisfaction about how the NHSCFA has dealt with a situation, claims that a poor standard of service has been provided and claims that NHSCFA staff have been unhelpful or rude. The NHSCFA Complaints process comprises of an electronic log of informal and formal complaints consisting of an Excel spreadsheet containing personal and sensitive information, and is held in a restricted access area, with the corresponding material stored in a restricted Teams folder. Additionally there is an Outlook folder, again with restricted access, for email communication in which online reporting forms are also received.

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

NHSCFA leads on a wide range of work to protect NHS staff from economic crime. The purpose of the NHSCFA Complaints Process is: to facilitate a satisfactory response on behalf of the CFA to complaints raised by the public, and to resolve the complaint for the complainant, ensuring we are providing an effective, consistent, high standard complaints process to the public, providing them with the opportunity to resolve the matter(s) they have brought to the attention of the CFA. Access is restricted to 2 members of staff within NHSCFA, including the database administrators.

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

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the NHSCFA Complaints Process has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

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

This is the first DPIA carried out on the system, and replaces the original NHS PROTECT PIA - Complaints Process 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

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

London

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

Newcastle

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