NHS
Counter Fraud Authority

Public website (cfa.nhs.uk)

Data Protection Impact Assessment

November 2019

V1:0

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

Executive Summary

This document contains information in relation to the NHSCFA's public website (cfa.nhs.uk).

The system is the public facing website for NHSCFA.

The website provides access to information and updates from NHCFA for stakeholders and members of the public. The website is also used to collect data which is appropriate for preventing and detecting crime within the NHS, ensuring that personal data is adequate, relevant and not excessive for the purposes for which it is processed.

Data is collected through the freedom of information requests and through data collected in the form of subscriber consent to be contacted by NHSCFA.

This document is deemed OFFICIAL and 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'**

Table of contents

Executive Summary **2**

Links & Dependencies **5**

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

Introduction 6

Name of Database /System general Description 7

Data Protection Impact Assessment 7

Ownership 19

2. DPIA Report **19**

Section 1: Overview of Data Collection and Maintenance 19

Section 2: Uses of the Application and the Data 20

Section 3: Data Retention 20

Section 4: Internal Sharing and Disclosure of Data 20

Section 5: External Sharing and Disclosure of Data 20

Section 6: Notice/Signage 21

Section 7: Rights of Individuals to Access, Redress and Correct Data 21

Section 8: Technical Access and Security 21

Section 9: Technology 21

3. Compliance Checks **22**

DPA 2018 Compliance Check 22

The Privacy and Electronic Communications Regulations 22

The Human Rights Act 22

The Freedom of Information Act 22

Conclusion 22

Annex A - Definition of Protected Personal Data 23

Annex B - Data Protection Compliance Check Sheet 24

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Helen Fox	DPIA / public website	Trevor Duplessis	V0.1	01/11/2019	Initial template completed
Helen Fox	DPIA / public website	**T**revor Duplessis	V1.0	12/11/2019	Review, amendments and sign off.

Prefix	
Reference:	**DPIA / public website**
Date:	**November 2019**
Author:	**Helen Fox / Niall Marsh**
Data Owner:	**Purdy Sian Davis**
Version:	**1.0**
Supersedes	**0.1**

Links & Dependencies

Document	Title	Reference	Date	POC
Government Security Classifications	Government Security Classifications	All	April 2014	Cabinet Office
EU GDPR	EU General Data Protection Regulation	All	May 2018	GDPR
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
DPA	Data Protection Act	All	2018	HMG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG
HRA	Human Rights Act	All	1998	HMG
FOI	Freedom of Information Act	All	2000	HMG

1. Data 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.

Name of Database /System general Description

10. The website provides access to information and updates from NHCFA for stakeholders and members of the public. The website collects data from the freedom of information requests and through data collected in the form of subscriber consent to be contacted by NHSCFA.

11. CFA.NHS.UK is a Java 8 Spring Boot MVC web application hosted on an AWS cloud virtual server (based in London, UK) running a CIS hardened image of Unbutu 18. The application is database driven using MySQL 5.7 also hosted on a CIS hardened image of Unbutu 18. The website consists of several interactive html form elements that collect personal identifiable data for the purposes of processing general enquiries, direct marketing and subscriptions to news and information services where explicit consent has been obtained, service improvement and quality assurance and data and information requests.

12. The CFA web application is a database driven content management system (CMS). For security and confidentiality purposes, database systems that underpin the CFA website are only accessed by approximately up to 10 members of authorised staff from NHSCFA, which includes the database administrators.

13. This is the only DPIA to be completed on the public website and it has been carried out by the Information and Records Management Officer, in consultation with the Corporate Communications and Engagement Lead, Web Application Development Specialist and the Information Governance and Risk Management Lead.

14. The public website, 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 the public website 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

STEP 1: Identify the need for a DPIA

[2] Version 0.3 (20180209)

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 NHSCFA public website collects data from the freedom of information requests and through data collected in the form of subscriber consent to be contacted by NHSCFA. We use information provided or held about you in the following ways: • to provide you with information about our guidance or services that you request from us, where you have consented to be contacted for such purposes • to improve our website to ensure that content is presented in the most effective manner • to allow you in to participate in some of the interactive features of our service when you choose to do so • to notify you about changes to our service(s) You have the right to ask us not to process your personal data or share it with other organisations (subject to certain exceptions). We will usually inform you before collecting your data, if we intend to disclose your information to any third party. You can exercise your right to prevent such processing by checking the relevant tick boxes on the forms or data portals we use to collect your data.

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?

Data is collected:

- through any user information that is given through the freedom of information and the contact us form
- Through subscriber data via MailChimp
- if you contact us, we may keep a record of that correspondence or telephone call.

Personal data is collected typically from the data subject themselves as part of their regular use of the System via an online system.

Subscriber data containing contact name and email addresses will be shared via secure electronic transfer to our third-party processor (MailChimp) who process bulk and email marketing campaigns on our behalf.

We are not processing information which is deemed as ‘likely high risk’ are involved.

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?

The processing of personal information and the protection of individual rights is governed by both the General Data Protection Regulation (GDPR) and Part 2 and/or Part 3 of the Data Protection Act 2018. The primary purpose for processing your personal data determines what law protects your rights and provides the legal basis for our processing activities.

Where the NHS Counter Fraud Authority (NHSCFA) processes your personal data for general purposes not relating to the organisation's statutory function, the GDPR and Part 2 of the Data Protection Act 2018 apply.

The nature of the data is personal contact information only.

We will be collecting the minimum amount of data required to fulfil the request of the enquiry.

Data will only be collected at the time a request is made or a subscription is registered.

The NHSCFA's lawful bases for processing the types of personal data below fall within the following permitted categories through public task and consent.

Correspondence and contact with the NHSCFA for general purposes connected with its statutory function.

The number of individuals affected are unknown and could range from 200 to 1,000 people.

It has a global reach, although data collected and processed will be done so via user information.

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)?

You have the right to ask us not to process your personal data or share it with other organisations (subject to certain exceptions). We will usually inform you before collecting your data, if we intend to disclose your information to any third party. You can exercise your right to prevent such processing by checking the relevant tick boxes on the forms or data portals we use to collect your data.

The NHSCFA shares data with other public bodies under Memorandums of Understanding (MOUs) and Information Sharing Agreements (ISAs). These enable cooperation and information sharing between public bodies. Our current list of MOUs and ISAs are available on the Who we work with page.

We may also share data:

- if we are under a duty to disclose or share personal information in order to comply with any legal obligation,
- for the prevention of crime, in accordance with the law, with regulatory or governing bodies,
- with analytics and search engine providers that assist us in the improvement and optimisation of our website. Please note that we do not disclose information about identifiable individuals to such third parties, but we may provide them with anonymous aggregate information about visitors and users,
- those interacting with us on social media.

Users are providing data that they wish NHSCFA to process.

All data that we collect and any information that you provide to us is safely stored on our servers, which are encrypted through a secure system. No data is stored or transferred outside the European Economic Area (EEA). We use industry best practice and standards.

The DPA and the GDPR set the rules for disclosure of personal details. Every living individual has the right to request access to their own personal data. To request your personal data you must make a subject access request; this can be done via email to: DPArequest@nhscfa.gsi.gov.uk.

For more information on subject access requests, please see the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

If you have a concern about the organisation's information rights practices, you have the right to make complaint to the ICO or another supervisory authority.

There are currently no issues of public concern.

The NHSCFA abides by legislation on data sharing, for example the DPA and the GDPR, which sets rules for the handling personal data, and the Human Rights Act and the common law duty of confidentiality, which protects confidential and private information (subject to certain exceptions). For further information see the

following:

- Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- General Data Protection Regulation: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- Human Rights Act 1998: http://www.legislation.gov.uk/ukpga/1998/42/contents
- The Common Law Duty of Confidentiality: http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/browsable/DH_5803173

- ISO120000-1 and ISO27001 information and security management

Digital online Freedom of Information request forms are common place throughout public sector organisations and is stated as a contact method on .GOV.UK https://www.gov.uk/make-a-freedom-of-information-request/how-to-make-an-foi-request for the submission of these types of requests. Mail subscription services and online signup and opt in services are common place throughout the web. Mailchimp is the market leader in this technology.

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?

We use information provided or held about you in the following ways:

- to provide you with information about our guidance or services that you request from us, where you have consented to be contacted for such purposes
- to improve our website to ensure that content is presented in the most effective manner
- to allow you in to participate in some of the interactive features of our service when you choose to do so
- to notify you about changes to our service(s)
- to allow the organisation to provide an improved service user focused, streamlined service, with better analytical capabilities

The intended effect is for people to be more engaged, better informed about the work of the organisation. The public website enables users to get in touch with NHSCFA in different ways and report fraud.

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?

The public website has been upgraded and shared internally with NHSCFA.

We have engaged internally with experts who provide assistance with the development and roll out of this system.

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?

The NHSCFA's lawful bases for processing the types of personal data below fall within the following permitted categories of public task and consent. It requires users to fulfil the requests.

The way data is processed uses the best method for fulfilling FOI requests and managing a user's subscription to our services.
Other processes for collecting data would be a manual process of emails and posts. The online forms have been developed to collect the minimum amount of data to enable the current process.

Validation rules are used in the collection of data.

The proposed processing does actually achieve our purpose, as demonstrated by the current NHSCFA website, which involves very similar processing.

Information given to individuals will all relate to the work of NHSCFA. Information given and a person's rights is aligned to the terms of conditions, the website privacy notice and organisational policies.

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, unless new applications are activated. If we do look into activating new applications, we will update this assessment to reflect this.

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
System used for intranet is compromised or loss of personal data which includes name, address and telephone numbers and organisation names where provided.	Possible	Significant	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 Yes/No
The CFA website has many security layers in place to ensure the security and protection of personal data. The core application is secured using Spring Security and built on standard Spring Boot MVC practices. The application sits behind several firewalls and reverse proxy server as well as a web application firewall or WAF. 128bit TLS1.2 encryption is used to secure network connections between the application server and the MySQL database server and the application server and the client. Similar encryption with basic authentication (user id and key) is also used to secure the transfer of data between this service and our third-party mail service provider MailChimp.	Reduced	Medium	

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:	Trevor Duplessis 13 November 2019	If overruled, you must explain your reasons
Comments: I am satisfied having reviewed the DPIA that a comprehensive assessment has been undertaken of the system. Access to the software system is restricted to limited numbers of NHSCFA staff with limited and defined access by Mailchimp staff for analytical purposes only. Individual account access ensures the system is fully auditable and can be removed when no longer required. Personal information collected and processed by the system will not include special category or criminal offence data and will be subject to periodic review to ensure that it is not kept longer than is necessary in the accordance with the law and the organisation's data retention policy.		
Consultation responses reviewed by:		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 public website roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Purdy Sian-Davis
Senior Responsible Officer (SRO)	Richard Hampton
Application/Database Owner	Helen Fox
Data Protection Officer	Trevor Duplessis

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. The system will be a public website for the NHSCFA.
2. Data is collected through the freedom of information requests and through data collected in the form of subscriber consent to be contacted by NHSCFA and if you contact us, we may keep a record of that correspondence or telephone call.
3. The impact level of the public website Database /System was assessed as CONFIDENTIAL.
4. The following measures briefly describe what controls have been implemented to protect the public website Database/System and the personal data recorded:
    a. All off site back-ups are secure as they can only be opened via the encryption key
    b. The Database/System is only accessed by approximately up to 10 members of staff from NHSCFA, which includes the database administrators.
    c. The public website Database/System does not have any direct interconnections with other NHSCFA systems and applications.
    d. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.
5. It is assessed that there are no residual privacy risks to the personal data used by the public website
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. Describe the purpose of the Database/System.

8. The database application and associated servers and network infrastructures supporting the database are administered internally by NHSCFA database administrators and developers within the Information Systems Analytics (ISA) team.

9. Information in the Database/System could include; name, addresses, email addresses, telephone numbers, and organisation names.

10. No sensitive data is collected or processed within this system,

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

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

b. [The Database/System] does not have a direct interconnection with other NHSCFA systems or applications*)*

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

Section 3: Data Retention

12. The public website Database/System is subject to NHSCFA Data Handling and Storage Policy. There are no paper records involved with the processing of data within the public website. FoI requests are subject to standard deletion and retention policies. Subscriber data is deleted through an unsubscribe function provided to and instigated by the data subject.

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 up to 10 members of staff within NHSCFA including the database administrators.

Section 5: External Sharing and Disclosure of Data

15. The only information shared with external organisations, would be with the police if it was requested for the administration of justice and [if shared with other organisations need to state/confirm this is being done in accordance with appropriate Information Sharing Agreement/Memorandum of Understanding]

Section 6: Notice/Signage

16. Is the data subject aware that we hold the data for them? If not why not?

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

17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this Database/System and therefore outside the scope of this DPIA. Additional information on how the NHSCFA collect handle and process data can be found within the public websites privacy policy.

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 we only collect the minimum amount of data required to process the users request. Users also have the option to remove themselves from our mailing lists at any point.20. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

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

Section 8: Technical Access and Security

22. The security and technical access architecture of the 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 CESG approved IT Security Health Check.

23. Access is restricted to internal staff only.

24. The technical controls to protect the database include:

a. Anti-virus protection;

b. Permission based access controls to shared drive.

c. Logging, audit and monitoring controls.

d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

25. The Database/System holds personal information taken both by telephone and electronically and is located within the NHSCFA UK based AWS cloud infrastructure.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the public website, 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.

The Database does not process sensitive personal data.

The Privacy and Electronic Communications Regulations

4. 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

5. 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

6. 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

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

Annex A - Definition of Protected Personal Data

Personal data processed in the database includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, include:

Name;
Address;
Telephone number;

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual:

None processed

C. Sensitive personal data relating to an identifiable living individual:

None processed

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

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

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA
Project	Public website

2. Contact position and/or name, telephone number and e-mail address.
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

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

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

The system is the public website for the NHSCFA.

Data is collected through the freedom of information requests and through data collected in the form of subscriber consent to be contacted by NHSCFA and if you contact us, we may keep a record of that correspondence or telephone call.

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

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

The purpose of the Database/System is the public website.

Access is restricted to up to 10 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 public website has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

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

This is the first DPIA carried out on the system

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

*IMPORTANT NOTE: 'Personal data' means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Page left intentionally blank.

NHSCFA offices

Coventry

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

02476 245500

London

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

0207 895 4500

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH

0191 204 6303