NHS
Counter Fraud Authority

Stealthbits – Data Governance Solution

Data Protection Impact Assessment

June 2021

V1.0 Published Version

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

Executive Summary

This document contains information in relation to (**Stealthbits** – Data governance access solution which includes StealthAudit, StealthDefend StealthIntercept)

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 (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					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Security and Operational Support Specialist	DPIA Stealthbits	DPO	V0.1	June 2021	Initial creation
Security and Operational Support Specialist	DPIA Stealthbits	DPO	V1.0	June 2021	Final Approved

Prefix	
Reference:	**DPIA (Stealthbits)**
Date:	**June 2021**
Author:	**Security and Operational Support Specialist**
Data Owner:	**Information Security Team**
Version:	**1.0**
Supersedes	**0.1**

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
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.

Stealthbits – General Description

10. Stealthbits Data Access Governance solution (**StealthAudit, StealthDefend, StealthIntercept**) discovers where data lives and monitors who has access to it resulting in effective governance that promotes security, compliance and operational efficiency. The system is accessible only to Information Security Team members.

11. The Data Access Governance solution comprises of following stages behind the scenes –
Discover – where data resides
Collect & Analyse – relevant data points
Monitor – understand user interactions with data
Restructure – access to achieve least privilege principles
Govern – ongoing access to ensure security, compliance and operational efficiency.

12. This is the first DPIA to be completed on the system and it has been carried out by the Information and Records Management Officer, in consultation with Security & Operational Support Specialist and the Information Governance and Risk Management Lead.

13. The Stealthbits solution 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 Stealthbits solution 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.

Stealthbits is a data access governance solution comprising of 3 modules, as indicated below.

1) **StealthAudit** – Reporting and Governance solution.

   It automates the collection and analysis of the data from critical IT Assets including data, directories and systems (Active Directory, SharePoint, OneDrive, Exchange)

2) **StealthDefend** – Threat Detection & Response

   Detect and respond to abnormal behaviour and advanced attacks against active directory and file systems with accuracy and speed.

3) **StealthIntercept** - Monitor and prevent unwanted and unauthorised activities in real-time for Active Directory security and compliance.

It was identified that a DPIA was required, in knowing that the solution was likely to include the collection and analysis of personal and sensitive data.

STEP 1: Identify the need for a DPIA

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. Stealthbits uses its own SQL Server database for storing information which contains which user has access to what folders, which user has what kind of permissions and what type of sensitive information is being held in those stores/documents

2. Source of the data is from different stores such as Active Directory, Exchange, OneDrive, SharePoint

3. Data won't be shared anyone outside of the Organisation. Reports are being produced on a daily basis to do a sanity check of the permissions and the information contained.

4. High risk/ sensitive data would be picked up by the solution and would likely include National Insurance Numbers, NHS Numbers, Passport Numbers or Credit Card data

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. Nature of the data will involve information stored by the respective teams (NIS, CIU, FCU) etc and as such, will include special category and criminal offence data.

2. Data is collected on a continuous basis which applies to all the NHSCFA Staff

3. Data is collected on a continuous basis.

4. The data retention period will be set to one year.

5. This applies to all NHSCFA staff

6. It will cover England and Wales

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. The relationship is with NHSCFA Staff

2. Staff have no control

3. All NHSCFA Staff when onboarding have to agree to the Acceptable Use Policy

4. No

5. No

6. No, the solution is well established in business.

7. Many organisations are using this solution for data governance.

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. Data access governance solution StealthAudit makes sure who has access to what (data access subject reviews) and Stealth Defend for Threat Detection & Response. StealthIntercept audits and blocks any AD change requests, changes or authentications.

2. None

3. High Level understanding of Data Access at a Granular level.

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. This is not relevant.

2. Security Team have been involved in the implementation.

3. N/A

4. Solution implemented by internal security experts.

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. The lawful basis is (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

2. Yes

3. No

4. N/A

5. N/A – the solution only looks at the data

6. N/A

7. N/A – NHS staff agree to the Acceptable Use Policy

8. N/A

9. N/A – No International Transfers

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
NHSCFA Privileged User	Remote	Minimal	Low
Service Provider Privileged Users	Possible	Minimal	Low
Physical Intruder Data Centre	Remote	Minimal	Low
Internet Based Attacker	Remote	Significant	Low
Environmental (fire, flood, power supply etc)	Remote	Significant	Medium
Application Vulnerability	Remote	Minimal	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 by SMT Owner Yes/No
Environmental (fire, flood, power supply etc)	Accepted	Low	Yes

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by SMT Owner:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by SMT Owner:		If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.

Summary of DPO advice:

Having reviewed the DPIA I am satisfied that a comprehensive assessment of the data governance access solution Stealthbits, which locates, identifies and monitors data access in systems such as Active Directory, Exchange Online, SharePoint and One drive has been carried out. Overall system access is limited to be approximately 3 members of NHSCFA staff which includes he database administrators. Access will be fully auditable.

It is an industry recognised solution and 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.

Item	Name/date	Notes
DPO advice accepted or overruled by:	Trevor Duplessis - 30 June 2021	If overruled, you must explain your reasons

Comments:

Item	Name/date	Notes
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons

Comments:

Item	Name/date	Notes
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)	Information Systems and Analytics Manager
Senior Information Risk Owner (SIRO)	Head of Intelligence & Fraud Prevention
Application/Database Owner	Information Systems & Security Team
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The impact level of the Stealthbits 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 Stealthbits and the personal data recorded:

    a. The solution is accessed by approximately 3 members of staff from NHSCFA, which includes the database administrators

    b. The solution establishes direct connections to NHSCFA data source systems for example, Active Directory, Exchange Online, SharePoint and One Drive, in order to discover where the data lives and monitor who has access to it.

    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 Stealthbits.

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. Administration of the solution will be the responsibility of Information Systems and Security

6. The solution does not hold personal information but monitors access permissions, of which high risk data would include NI Numbers, NHS Numbers, Passport Numbers and Credit Card data

7. 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 Stealthbits Solution is subject to NHSCFA Data Handling and Storage Policy. The data retention period will be one year, and deletion will be automated once the threshold is reached.

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 solution is accessed by approximately 3 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. The data subject would be NHSCFA staff, who are all aware we hold their data.

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 solution 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 any access requests will be received as the personal data recorded is all in relation to access governance permissions of NHSCFA employees.

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 ISO27001

20. Access is restricted to internal staff only.

21. The technical controls to protect the database include:

a.   Anti-virus protection;

b.   Permission based access controls to shared drive.

c.   Logging, audit and monitoring controls.

d.   Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

22. The solution does not hold personal information but monitors access permissions 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 Stealthbits Solution, 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 Solution 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 solution. 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 Information Systems and Security
Project	Stealthbits – Data Governance Solution

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.

Stealthbits Data Access Governance Solution (StealthAudit, StealthDefend, StealthIntercept) discovers where data lives and monitors who has access to it resulting in effective governance that promotes security, compliance and operational efficiency. The system is accessible only to Information Security Team members

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 Solution is:

StealthAudit - Automate reporting and governance across dozens of platforms including File Systems, SharePoint, Office 365, One Drive, and Exchange.

StealthDefend - Detect and respond to unusual file access and activity which could indicate insider threats or advanced account takeover attacks using user behaviour analytics.

StealthIntercept - Prevent attempts to compromise AD security like unauthorised LSASS injection, NTDS.dit database extraction, and modification of AdminSDHolder container rights.

Access is restricted to Information Security 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 Stealthbits Solution 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	**London**	**Newcastle**
Earlsdon Park	4th Floor	1st Floor
55 Butts Road	Skipton House	Citygate
Coventry	80 London Road	Gallowgate
West Midlands	London	Newcastle upon Tyne
CV1 3BH	SE1 6LH	NE1 4WH