NHS
Counter Fraud Authority

GovDelivery

Data Protection Impact Assessment

2023

V1.0 approved

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

Executive Summary

This document contains information in relation to the GovDelivery.

GovDelivery is an 'email marketing' platform. It is an online tool used to target emails at large audiences. It will enable NHSCFA to segment email recipient lists based on various factors. Along with this the platform is able to provide reports on who has or has not interacted with the email, and how.

GovDelivery will contain a list of our stakeholders (Local Counter Fraud Specialists, Directors of Finance, Audit Committee Chairs and Fraud Champions). The information stored on the platform will have information such as email address, names and the organisations they're linked to and the type of organisation that is.

This document is deemed OFFICAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications.

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

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Senior Corporate Communications Officer	DPIA / GovDelivery	DPO	V0.1	June 2023	Initial template completed
Senior Corporate Communications Officer	DPIA / GovDelivery	DPO	V1.0	Dec 2023	Approved

Prefix	
Reference:	**DPIA GovDelivery**
Date:	**2023**
Author:	**Senior Corporate Communications Officer**
Data Owner:	**Corporate Communications Manager**
Version:	**v1.0**
Supersedes	**V0.1**

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 effect 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 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.

GovDelivery / Email marketing/delivery platform

10. GovDelivery is an email delivery platform used to send targeted communications to selected audiences.

11. Data being loaded onto GovDelivery will be extracted from CPOD (NHSCFA's counter fraud stakeholder's database) via SAS VA (web-based visual analytics environment). The data being extracted is contact information for counter fraud professionals in NHS providers (including some independent providers of NHS services), NHS commissioners, as well as arm's-length bodies and other organisations in the wider health group. The use of GovDelivery will generate user activity data, which will be used to help improve our messaging.

12. For security and confidentiality purposes, the platform is only accessed by approximately 20 members of staff from NHSCFA, which includes the administrators. Access will be permission-based.

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

14. The platform, in addition to GDPR is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

15. To ensure that GovDelivery 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.
GovDelivery is an e-mail delivery platform, that will enable us to target emails at the various stakeholders. The platform will also enable us sign up new subscribers to NHSCFA newsletters and keep up to date with all the latest news and developments across the NHS fraud community. Contact's name, email address, organisation and type of organisation will be the information saved onto the platform which requires a DPIA. Where people work from their homes their personal IP addresses will be collected.

STEP 2: Describe the processing

Describe the nature of the processing:

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

2. What is the source of the data?

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

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

1. Data is already held on other systems such as CPOD as required for the nominations process, etc. The data required will be placed on GovDelivery. GovDelivery will monitor user interaction with emails on our behalf. Periodically we will review our data to ensure all data held is up to date and valid.

2. Data will be from our contacts database CPOD and from the sign-up form provided on our website.

3. (Internally) Data may be shared with colleagues if required. This will be in the format of reports on the email activity (opened, clicks, clickthrough's) which will be used to target follow up messages.

4. GovDelivery records user information such as geographical location, IP address, and device/operating system used, this information helps us cater to our audiences better. The information sent are notices, circulars and updates. This enables the system to produce analytics for us, and all users will be informed of this before signing up to the system.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?

2. How much data will you be collecting and using?

3. How often?

4. How long will you keep it?

5. How many individuals are affected?

6. What geographical area does it cover?

1. The data is relating to our stakeholders at various organisations as detailed above. It includes information such as name, emails, work organisation. The system collects analytics for reporting purposes, this may include data such as device used to open email, geographical location of individual. It does not include special category or criminal offence data.

2. Roughly 2,000 contacts initially.

3. Contact data will be updated on a regular basis using data held on CPOD. On average once a week. This is a manual process where data is extracted from CPOD via a SAS report into a spreadsheet and uploaded to GovDelivery.

4. Data will be kept on the system while the user is active in their role. Users can request to unsubscribe from our mailing lists where we're contacting them using consent as a basis.

5. 2,000

6. 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 there 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. Stakeholders who have an interest in our area of work and have subscribed to our newsletters. Other contacts we have a responsibility as an authority to communicate with. We are using Public Task as a legal basis to contact those individuals. Users who voluntarily sign up to our newsletter will be under consent.

2. Users have a requirement to receive our communications to perform their duties. While we have various types of communications, they do have the option to opt out of content not necessary for them to perform their role. Users who wish not to receive any communications can choose to do so. We will email users as well as use the GovDelivery system to ensure that we are reaching everyone.

3.Yes

4.No

5.To my knowledge, no concerns have been raised regarding this type of processing, as it is a fairly well-established email marketing tool, available through many different providers.

I have no knowledge of any security flaws, however as this is a hosted solution, we have no control over the physical security measures in place. For this we rely on the certifications the supplier has achieved, such as ISO27001, for assurance of the security measures physically in place

6.No

7.Fairly well-established email marketing tools, available through many different providers.

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. Improved awareness within the NHS sector via the local NHS LCFS Community

2. Enabling them to perform their roles effectively by providing guidance, alerts, information, without any negative effects.

3. Easier to reach our audience. Better insight into what they respond positively to, enabling us to refine our communications.

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. We'll continue to seek feedback via email. We already communicate with our stakeholders via email, this tool will assist us in providing that service

2. We will continue to involve our internal customers i.e. teams sending communications out, the Digital team and the Information Security team.

3. We have engaged regularly with the supplier, who provide assistance on development and rollout of the system, and sought assurance from them on various aspects of data processing (e.g. location of data centres).

4. We have consulted with our Information Security team, and a demonstration was arranged for all of SMT/LT to attend. – members of IT, Governance, operations all attended.

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 – email recipients have an interest in our work and have subscribed to receive information about it.

2. Yes

3. No

4. State/Define beforehand how the service and data will be used. Our current process for registering contacts on GovDelivery is to extract a report from CPOD, this data is filtered to ensure only relevant data remains, before being uploaded to the GovDelivery platform.

5. A process is in place within the nominations team to review data on quarterly and biannual basis as well as on-going updates when notified. Email bounce backs are investigated. We regularly remove any data which is no longer required e.g. people leaving their role.

6. Individuals will be informed about personal data held on the platform and about processing through communications sent in advance of live release – this information will be available on the extranet at all times, and contact information will be provided for any queries or support required. Each communication will contain a standard footer explaining this as well. Individuals can make requests to the NHSCFA by a subject access request. This is considered by the Information Governance team and a decision is made on what information to release. How we handle personal data, our legal basis for processing and who we work with and may share data with is outlined in our website's privacy policy

7. Enable simple unsubscribe process. Adhere to a clear statement on how data is processed and managed along with an email footer stating why they're receiving the email. Support users in deleting their profiles if no longer required

8. GovDelivery is ISO27001:2013 certified.

9. UK based company with servers in UK. No transfers of data are expected outside the EEA.

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
Data Breach	Possible	Significant	Medium
Data being shared with third parties by the processor	Remote	Significant	Low
Account compromised	Possible	Severe	High

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
Data Breach – Limit the data stored on the system. Account Compromised – Limit the number of users who have access to the platform to only those who require it. Management of active user profiles. Explore enabling 2-factor authentication.	Accepted Reduced	Medium Medium	

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Comms Manager IGRML	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Risk Register Review Group escalated for approval by SMT which was agreed and minuted on 13.12.23	If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice: all areas reviewed, including the Q&A amendments and the option to opt out.		
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 GovDelivery 'email marketing platform has been undertaken. The platform is an online tool used to target emails at subscribers. To do so, the platform collects contact name, email address, organisation and type; where individuals work from home, their IP address, location details, as well as any electronic devices and the software used to view these materials will be collected. Access to personal data will be limited only to those requiring access to the analytical output(s), with plans being considered to introduce additional protection via multi-factor authentication. Action has been taken to mitigate the associated inherent risk so far as possible with NHSCFA having discussed at the RRRG agreeing to carrying the residual risk. There are appropriate organisational measures in place to ensure personal data is held safely and securely, and that it is held in accordance with current legislative data protection requirements, organisational best practice and its data retention policy. I am therefore satisfied with the organisational security measures employed.		
Consultation responses reviewed by:	IGRML 18th December 2023	If your decision departs from individuals' view, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:	Corporate Communications	The DPO should also review ongoing compliance with DPIA

Ownership

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

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Corporate Communications Manager
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Senior Corporate Communications and Engagement Officer
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. GovDelivery is an 'email marketing' platform. It is an online tool used to target emails at large audiences. It will enable NHSCFA to segment email recipient lists based on various factors. Along with this the platform is able to provide reports on who has or has not interacted with the email, and how.

2. The platform will contain a list of our stakeholders (Local Counter Fraud Specialists, Directors of Finance, Audit Committee Chairs and Fraud Champions). The data stored will be information such as email address, names and the organisations they're linked to and the type of organisation that is. The platform itself records information on user interaction with the communications, by recording times email was accessed, along with location and device used. Where people work from their homes their personal IP addresses will be collected.
3. The impact level of GovDelivery was assessed as CONFIDENTIAL, and it can only be accessed internally.
4. The following measures briefly describe what controls have been implemented to protect GovDelivery 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 platform is only accessed by approximately 20 members of staff from NHSCFA, which includes the administrators.

c. GovDelivery does not have any direct interconnections with other NHSCFA systems and applications. Our current process for registering contacts on GovDelivery is to extract a report from CPOD, this data is filtered to ensure only relevant data remains, before being uploaded to the GovDelivery platform.

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. Any residual privacy risks to the personal data used by GovDelivery have been highlighted in the Risk Assessment Report

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

Section 2: Uses of the Application and the Data

7. GovDelivery is an 'email marketing' platform. It is an online tool used to target emails at large audiences. It will enable NHSCFA to segment email recipient lists based on various factors. Along with this the system is able to provide reports on who has or has not interacted with the email, and how. It is a recognised platform used by a range of public sector organisations.

8. GovDelivery will be administered by the Senior Corporate Communications and Engagement Officer and Corporate Communications Officer.

9. Information on the Platform could include; Contact's name, email address, organisation name, organisation type, region, role, location emails accessed from, IP address, time and date emails accessed and the type of device the emails were accessed from.

10. No sensitive data will be processed

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

a. Access is restricted to approximately 20 members of staff within NHSCFA including the administrators of the platform

b. The 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. Data held in GovDelivery is subject to NHSCFA Data Handling and Storage Policy, and will be retained as long as the user is active in their role. There are no paper records involved in the processing of data.
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 20 members of staff within NHSCFA including the administrators.

Section 5: External Sharing and Disclosure of Data

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

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 platform and therefore outside the scope of this DPIA.

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

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

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 GovDelivery is as explained in this DPIA:

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

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

c. Logging, audit and monitoring controls.

d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

25. The platform holds personal information. This information is extracted from CPOD via SAS and is located in the NHS Counter Fraud Authority data centre. Before the data is uploaded onto GovDelivery, it is reviewed and formatted to ensure only data required is being transferred to GovDelivery.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that GovDelivery, 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 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. While the platform would be considered an email marketing tool, we don't use it for marketing. Our recipients are subscribed to received updates on counter fraud activities.

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. Any residual privacy risks to the personal data used by GovDelivery have been highlighted in the Risk Assessment Report. 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: Corporate Communications
Project	GovDelivery

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)

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.

Email delivery platform used to send targeted communications to selected audiences.

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

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

The purpose of the platform is to deliver communications from the NHSCFA to our stakeholders and counter fraud professionals in the NHS.

Access is restricted to 20 members of staff within NHSCFA, including the administrators.

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

Data Protection Impact Assessments (DPIA) are considered in the light of personal data gathered, and the data in the GovDelivery platform will be 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 platform

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
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH