NHS
Counter Fraud Authority

Email Security Gateway

Data Protection Impact Assessment

July 2018

V0:3

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

Executive Summary

This document contains information in relation to the Email Security Gateway

The purpose of the Gateway is to control the flow of emails in and out of the NHS network in order to prevent unwanted, malicious and infected emails from being delivered. It facilitates the sending and receiving of external emails whilst also keeping a log of everything that passes through.

Rules are configured to stop any unwanted, malicious and infected emails with email content being automatically examined against the ruleset to determine the action taken.

The emails could contain any type of personal or sensitive data and a copy of each one is stored temporarily on the gateway and either released or deleted depending on whether they are safe.

When 75% of the total storage is reached the oldest emails are automatically removed.

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 (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 6

1. Data Privacy Impact Assessment Requirement & Process 7

Introduction 7

Email Security Gateway 8

Data Protection Impact Assessment 9

Ownership 20

2. DPIA Report 21

Section 1: Overview of Data Collection and Maintenance 21

Section 2: Uses of the Application and the Data 22

Section 3: Data Retention 22

Section 4: Internal Sharing and Disclosure of Data 23

Section 5: External Sharing and Disclosure of Data 23

Section 6: Notice/Signage 23

Section 7: Rights of Individuals to Access, Redress and Correct Data 23

Section 8: Technical Access and Security 23

Section 9: Technology 24

2. Compliance Checks 24

DPA 2018 Compliance Check 24

The Privacy and Electronic Communications Regulations 24

The Human Rights Act 24

The Freedom of Information Act 24

Conclusion 25

Annex A - Definition of Protected Personal Data 26

Annex B - Data Protection Compliance Check Sheet 27

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Susan Hyde	DPIA/ Email Security Gateway	Trevor Duplessis	V 0.1	05/07/2018	All
Susan Hyde	DPIA/ Email Security Gateway	Trevor Duplessis	V 1.0	16/10/2018	Minor – page 7
Susan Hyde	DPIA/ Email Security Gateway	Trevor Duplessis	V 2.0	31/03/2019	Redacted to prevent security risks to the organisation when published
Susan Hyde	DPIA/ Email Security Gateway	Trevor Duplessis	V3.0	11/11/2019	Final review and redaction.

Prefix	
Reference:	**DPIA Email Security Gateway**
Date:	**July 2018**
Author:	**James Ogilvie / Connor Gilroy**
Data Owner:	**Rosie Mullen**
Version:	**3:0**
Supersedes	**2:0**

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 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 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.

Email Security Gateway

10. The purpose of the Gateway is to control the flow of emails in and out of the NHS network in order to prevent unwanted, malicious and infected emails from being delivered. It facilitates the sending and receiving of external emails whilst also keeping a log of everything that passes through.

11. The process used is that rules are configured within the system to stop any unwanted, malicious and infected emails being delivered, as the email content is automatically examined against the ruleset to determine the action taken.

It is configured to analyse and score emails as they are received to determine their Spam probability. Emails with a Spam score greater than 5 are automatically blocked. Emails that score between 2 and 5 are tagged with a [QUAR?] prefix in the Subject line and quarantined but can be released by the Service Desk if a false positive is found. Emails that score between 1 and 2 are tagged with a [SPAM?] prefix in the Subject line but are still delivered. This is to alert the recipient that the email might be Spam as it has a higher than average score.

12. The emails could contain any type of personal or sensitive data and a copy of each one is stored temporarily on the gateway and either released or deleted depending on whether they are safe.

When 75% of the total storage is reached the oldest emails are automatically removed.

13. For security and confidentiality purposes, the database is only accessed by approximately 9 members of staff from NHSCFA. This includes IT Administrators and Service Desk staff who have individual accounts to access the system. Access is required to resolve faults, correct email delivery problems and to release incorrectly quarantined emails. Access to the system is requested via the Service Desk and once approved it's granted by an IT Administrator

14. This is the only DPIA to be completed on the Email Security Gateway and it has been carried out by the Information and Records Management Officer, in consultation with the Security and Operational Support Specialist, and the Information Governance and Risk Management Lead.

15. The Gateway, 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

16. To ensure the Database/System meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template[2] comprised of seven steps:

Step 1 - Identify the need for a DPIA

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

Step 7 - Sign off and record outcomes

[2] Version 0.3 (20180209)

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The Email Security Gateway include two clustered devices, and is used to:

- Control the flow of emails in and out of the NHS network
- Rules are configured to stop unwanted, malicious and infected emails from being delivered
- Email content is examined against the ruleset to determine the action taken

The system was only deployed in March 2018, with the system it replaced (ProofPoint) having been in place for over 6 years. As such, It was decided that a DPIA was required, in order to document what data was being processed in comparison to the previous system and to determine the justification.

The type of data that can be processed by this service includes personal and sensitive information as well as information that does not fall into either of the above categories. It depends on what information is being sent as the email system itself does not have any limitations on what information a user can enter. The majority of the processing will be automated as the gateway will analyse the contents of the email, including attachments, and compare them to categories it has been set to protect against such as phishing. The Service Desk have access to the Sender, Receiver and Subject and will process emails that score between 1 and 2 out of 10. A systems administrator would have full access to the email contents.

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?

A copy of every email that is processed by the Email Security Gateway is automatically stored on the gateway, and
the emails are stored temporarily and would not be opened unless they needed to be analysed in order to determine if safe to allow through.

When emails are received they're automatically checked by the system to see if they're legitimate and can be delivered or if they're likely to be malicious or spam and need to be quarantined. If they are legitimate they would be delivered normally, however if they're quarantined , the Service Desk will manually check to see if they've been quarantined correctly or if they're genuine and should be released.

Service Desk staff cannot see the actual message content, they can only see basic details such as sender, recipient, subject, date and time etc. The Service Desk have access to the message log which shows the email status ie delivered, quarantined and they can make a decision based on this.

The source of the data is inbound and outbound external emails, which are stored as a reference and for statistical analysis.

The email content is not shared with anyone and only IT Administrators can see it. The email body is blanked out for Service Desk staff.

The processing is not identified as high risk.

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 emails could contain any type of personal or sensitive data. However the content of the emails would not be routinely checked as they pass through, as the gateway is only there to control the flow of emails in and out of the NHS network, in order to stop unwanted, malicious and infected emails from being delivered.

All external emails are stored in the gateway during their cycle, however when 75% of the total storage is reached the oldest emails will be automatically removed.

This is a continuous process, where the data is kept temporarily and deleted in the order in which it was received once 75% of the total storage is reached.

There is no agreed time set by the vendor as to how long it might take for 75% storage to be reached as it would depend on the quantity of emails through the gateway.

All individuals who are sending or receiving external emails at given time would be affected. Therefore it would be impossible to quantify numbers.

All geographical areas would be included.

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)?

Any and all individuals making or having email contact with NHSCFA.

If persons contact NHSCFA via email, then it would be consensual and therefore they would have a degree of control. i.e: it is their decision to make contact or not.

We would not be examining data for example as per Step 2 above.

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?

To ensure that only genuine emails are delivered, in order to maintain integrity of the organisations email system and thus avoiding its compromise.

The intended effect is to make sure that unwanted, malicious and infected emails are not delivered.

The benefits of the processing are that by removing malicious and infected emails we will be keeping the network safe.

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 overall service itself has barely changed, the system used to provide it has. Due to this the stakeholders were not required to be made aware of the entirety of the change and were instead informed of the noticeable changes to the service, for example the quarantined mailbox.

The people involved from the organisation are the Service Desk, the IT Administrators and the Information Security team.

For this same reason consultation with information security experts is not required at this time as the service has not undergone a drastic change.

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 processing of data is lawful as the email gateway is specifically used to prevent malicious and potentially damaging email content from entering and leaving the organisation's network.

The defined lawful basis for the processing as identified in Article 6(1) of GDPR would be:
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.

The processing provides a safeguard and is a reliable solution for meeting the organisation's security objectives.

User training does provide a similar outcome to the email gateway as it reduces the likelihood of a successful email based attack. However this then allows for spam and malicious emails to impact work as users will have to spend more time trying to decide whether an email is a malicious email or not.

The email gateway works within a specific remit of data security and protection and follows a defined ruleset, function creep is not likely to occur.

Access to email content is restricted to IT administrators, the Service Desk staff are unable to see the body of emails that pass through the gateway. These restrictions ensure the data privacy, integrity and quality is maintained.

Staff automatically accept the IT Security Policy and Acceptable Use Policy upon signing into the NHSCFA Computer Systems. All staff are advised to read these documents upon their induction to the CFA and therefore should be aware of email communications being monitored.

By limiting the full access to emails to a select number of users we reduce the chances of a successful compromise of the system and access being gained to the staff emails. This also limits the impact of the insider threat by limiting the number of users who could cause actual damage to the service.

International transfers only occur when an email is sent or received from a mail server located outside of the UK. Any documents rated official-sensitive are encrypted using an encrypted email service.

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
NHS CFA Email Gateway User (Service Desk) – Through accident or intent a service desk user uses the service in a way that can cause damage to the organisation. The agent is unable to view the overall contents of the email therefore information disclosure risks are limited. Due to emails scoring between 2-4 being quarantined they are unlikely to be able to forward anything too damaging through (Such as known malware being attached to the emails).	Remote	Significant	Low
NHS CFA Email Gateway User (IT Administrator) – Through accident or intent an IT administrator uses the service in a way that can cause damage to the organisation. The administrator is able to view the contents of emails and therefore could perform data exfiltration. There is also the potential for the administrator to modify the rules on the service potentially allowing for more malicious emails to go through the email gateway.	Remote	Severe	Medium
Physical Intruders – Someone could steal the physical Gateway from the site. The Gateway stores emails on it potentially allowing for access to sensitive data alongside a denial of service as well. Security Controlled Entrance to the site where the Gateway is stored. Electronic passes are on all of the doors to the data centre.	Remote	Severe	Medium
External Attacker (Network) – As a results of a successful attack on our network from an external user they could gain access to the email Gateway. They would likely need to compromise one of the accounts on the Gateway, the fewer accounts with access to the Gateway and the fewer still with admin access the better.	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
Continual assessment of opportunities to improve network security. Continual monitoring of access rights given to staff and removal of access where it is no longer required. Integration of the Email Gateway logs into the current SIEM (Security Incident and Event Management) solution for use with pattern recognition and alerts.	Reduced Reduced Reduced	Medium Medium 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	N/A	DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Trevor Duplessis (DPO) 16th October 2018	If your decision departs from individuals' view, you must explain your reasons
Comments: I am satisfied that a comprehensive assessment of the system has been undertaken. Access to the database is restricted to small number of staff, who all have individual access account which can be fully audited. There is an automated review of retained materials built into the system once 75% total capacity is reached. Whilst this is not time specific and is dependent on the quantity of emails through the gateway, this is an area that will be subject to continuous assessment to improve the system. The Gateway of situated in a secure, security controlled site, with electronic passes on all doors to the data centre. This will enable auditable access to and from the site and therefore I am satisfied with the organisational security measures in place.		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Ownership

16. The following table describes the Email Gateway roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Rosie Mullen
Senior Responsible Officer (SRO) Information Risk Owner (IRO)	Richard Hampton Richard Hampton
Application/Database Owner	Simon Clark
Data Protection Officer	Trevor Duplessis

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. The email security gateway is a system used to control the flow of emails in and out of the NHS network, and to stop unwanted, malicious and infected emails from being delivered.

2. The data contained in the emails could include personal and sensitive information.

3. The impact level of the Email Gateway System was assessed as Official Sensitive and it can only be accessed internally.

4. The following measures briefly describe what controls have been implemented to protect the Email Gateway System and the personal data recorded:

    a. The gateway devices are housed in locked cabinets in the Skipton House Data Centre. There are two sets of doors with electronic access control systems. The NHSCFA Data Centre can only be accessed by authorised members of staff and building security.

    b. The System is only accessed by approximately 9 members of staff from NHSCFA, which includes the system administrators who monitor the system and ensure it remains fit for purpose and isn't being accessed by unauthorised staff or abused in anyway.

    c. The devices are located behind a "Next Generation Firewall owned and managed by NHSCFA.

    d. The next generation firewalls log all activity, the logs are analysed using the NHSCFA SIEM system, LogRhythm.

    e. Logical and physical related security incidents are reported to the Service Desk in the first instance. The ISA Information Security team are informed and they investigate them.

    f. The Email Security Gateway has direct links with the external mail relays on the PSN network and with the internal Data Loss Prevention system, gateway and SMTP server

    g. 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 Email Gateway System.

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 System.**

The purpose of the email Gateway is to find and filter Spam, phishing and other malicious emails. This is to help meet our security goals by reducing the chance of a successful email based attack.

8. **Who has responsibility for the administration of the System**

The information security team will perform user and rule based administration while the quarantine aspect of the service will be managed by the Service Desk.

9. **Information in the System could include;**

Emails sent to and from the organisation. Due to this they can include a wide variety of information such as –

Names

Job roles and tasks

Medical information

This is not an exhaustive list.

10. **Also list any sensitive data:**

Emails sent to and from the organisation. Due to this they can include a wide variety of information such as –

Medical Information

Sensitive information relating to ongoing cases

This is not an exhaustive list.

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

a. Access is restricted to approximately 9 members of staff within NHSCFA including the database administrators

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. The Email Gateway System is subject to NHSCFA Data Handling and Storage Policy. The emails are kept on the email gateway until it reaches 75% storage capacity. Upon reaching 75% storage capacity the gateway will begin deleting the oldest emails.

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 9 members of staff within NHSCFA including the System 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.

Section 6: Notice/Signage

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

NHS.CFA'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 System and therefore outside the scope of this DPIA.

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

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

19. It is unlikely that many access requests will be received as the personal data recorded is all in relation to email communications.

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 System holds personal information taken electronically and is located in the NHS Counter Fraud Authority data centre.

2. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the Email Gateway System, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

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

b. The Data Protection Principles;

c. The interpretations of the Principles.

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

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

4. The System processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, see Annex 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 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 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
Project	Email Gateway

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 system/technology 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 original system was the Trustwave Email Gateway service. This service performed checks on incoming emails in an attempt to filter Spam, Phishing and other malicious emails with the goal of reducing the chance of a successful compromise of our network via an email based attack.

The new system is a different Email Gateway service. This service performed checks on incoming emails in an attempt to filter Spam, Phishing and other malicious emails with the goal of reducing the chance of a successful compromise of our network via an email based attack.

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 System is:

To reduce the number of spam, phishing or malicious emails that reach the NHSCFA email users. This reduces the likelihood of a successful email based attack.

Access is restricted to 9 members of staff within NHSCFA, including the system administrators.

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

Dare Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the Email Gateway System 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 55 Butts Road Coventry West Midlands CV1 3BH	4th Floor Skipton House 80 London Road London SE1 6LH	1st Floor Citygate Gallowgate Newcastle upon Tyne NE1 4WH
02476 245500	0207 895 4500	0191 204 6303