Data Protection Impact Assessment for NHSmail users in Scotland

Published May 2018
Version 1

Contents

1. Introduction

This document is the Data Protection Impact Assessment (DPIA) for the NHSmail Live Service, providing details of how the NHSmail Live Service (and the expected use of the service by local organisations) aligns to the new regulations set out in the GDPR (General Data Protection Regulation) legislation.

The NHSmail Live Service is the secure email and collaboration service, available for use by all health and care organisations in England and Scotland, as approved by eHealth governance within Scotland via:

- Approval of the Full Business Case (FBC) in May 2015.

This DPIA is for all organisations based in Scotland – who are supported by NHS National Services Scotland (NSS). A separate DPIA is available for organisations based in England – who are supported by NHS Digital.

NSS is the Service Provider for the NHSmail Live Service, acting as a Joint Controller with local organisations based in Scotland. NSS is responsible for managing the data processing contract with Accenture (Processor) via a five-year contract (with end date of 31 March 2021). The terms and conditions set out in the contract, which have been uplifted in accordance with GDPR in April 2018 (Variation Notice 12), stipulate that data must be processed in accordance with:

- Data Protection Act (1998).
- UK Data Protection Bill (14 Sep 17).
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
- Working Party 29 guidelines determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, wp248rev.01.
- Data Protection Act (25 May 2018).

NHSmail core products are funded centrally via the NHSmail FBC, including:

- Secure Email account (users and shared mailboxes) – 4GB.
- Skype for Business (SfB) Instant Messaging and Presence (IM&P).
- NHS Directory (list of NHSmail users and contact details).
- Calendar Federation.
- Directory Federation.
- Address Book Federation.
- Skype Federation.

Local organisations can opt to procure additional services by signing a top-up service agreement with Accenture, including:

- Skype for Business (SfB) Audio and Video.
- Larger mailbox accounts (6GB, 25GB).

2. Consultation with Stakeholders

The NHSmail Live Service, which has been in place since 2002, now provides a secure email and collaboration service for all health and care organisations within England and Scotland, that choose to select NHSmail as their secure email platform.

The design of the NHSmail Live Service (in particular NHSmail2 which was procured in 2014), includes security and collaboration as the core features and were captured during the procurement phase following wide spread consultation by NHS Digital and on behalf of NSS:

- Workshops held with Chief Information Officers (CIOs), Royal Colleges and engagement with IT professionals via regional CIO forums.
- End user stakeholder groups.

The NHSmail Live Service contract between NSS (as Joint Controller with Scottish health and care organisations) and Accenture (Processor) sets out the conditions for the service design and the service level agreements (SLAs) that must be met. The contract was finalised following consultation with:

- NHSmail programme leads.
- Accenture programme leads.
- NSS, NHS Digital and Accenture legal and commercial teams.
- Department of Health.

Regular user group sessions are held with stakeholder groups to shape and refine the service provision including: monthly webinar with Local Administrators, annual all-user survey, user group workshops.

The NHSmail Live Service Access Policy sets out the user groups that are served and the Acceptable Use Policy (AUP) provides each individual using the service with details of the terms and conditions by which the service operates.

For NHSmail policy documentation and guidance visit the NHSmail Portal help pages: https://portal.nhs.net/Help/.

3. Description of the Processing

3.1 Summary

Category	**Who's information**	**System**	**Where is it going**	**Nature and Purpose of the Processing**	**Frequency** e.g. daily, weekly, monthly, real time	**Method of transport** Electronic system transfer, Fax, Secure Email, Paper or shared drive, Post	**PID/ No PID**	**Type of information** e.g. letter, report, referral or patient history
NHS Directory and metadata	Controller staff, Controller Service Recipient	NHSmail	Stored within NHSmail in the UK. May be viewed outside of the EU.	Administration of services provided by NHSmail	Real-time	Electronic system transfer - EST	PID	Business identifiers - email address, - telephone number - organisation First Name Last Name
Content Stored with NHSmail Services i.e. email, Skype message, etc.	Controller staff, Controller Service Recipient staff, NHS patients, member of the public	NHSmail	Stored within NHSmail in the UK. May be viewed or transmitted outside of the EU.	Processing and storage of email and other data.	Real-time	Electronic system transfer - EST	PID	Patient identifiable data which may include reports, medical images, passport detail copies, financial data, other personal identifiers.

3.2 Data Categories

The data processed by the NHSmail Live Service includes:

- Data controlled by the NHSmail Live Service e.g. Email account details, NHS Directory.
- Data shared or stored by local organisations using the NHSmail Live Service e.g. Email, Skype messages, SharePoint documents, etc.).
- Data shared with partner organisations via federation or partnership agreements e.g. NHS Directory, Calendars, Address Book.

Data processing falls into two main categories:

- Data processing by NSS, NHS Digital and Accenture to run and maintain the NHSmail Live Service.
- Data processing performed by local organisations using the NHSmail Live Service to share or store data (including patient identifiable data).

3.3 Data Processes

NHSmail accounts are set up for staff by local organisations (Joint Controllers) using the NHSmail Portal or TanSync. This data includes:

- Business identifiers
  - email address
  - telephone number

    - organisation information
- First name
- Last name

NHSmail users are able to share or store data (including patient identifiable data) using the NHSmail Live Service in accordance with local organisation policies and procedures. Users may share data through the NHSmail platform with other users within NHSmail or external recipients on the Internet, typically via email.

NHSmail also includes services providing email routing for local organisations, collaboration services with Office 365 and authentication services for third party applications.

Data processing guidance

The NHSmail Live Service (NSS, NHS Digital – Joint Controller) provides guidance and policy documentation on the running and maintenance of the service to inform local organisations (Joint Controllers) and their users.

Local organisations (Joint Controllers) are responsible for setting policies and procedures to govern the types of data that can be shared, with whom, with which countries / organisations and the ways in which NHSmail users send and receive data from other organisations / individuals / countries.

3.4 Data Flow

NHS Directory & NHSmail Portal

Accounts are typically created for users of the NHSmail services by their employing organisation, this will include the user's name and other contact details like email and telephone numbers.

This data will then be published in the NHS Directory and NHSmail Portal to be used by other users of NHSmail for collaboration purposes (i.e. email, instant messaging, arranging meetings, etc.).

This information may also be shared with third parties who are federated with the NHSmail platform (i.e. local councils or commercial organisations working with the NHS). This is only to be used for the purpose of collaborating with the NHS. Use of this data for marketing or other purposes is not permitted.

This data may also be accessed by NSS, NHS Digital, Accenture and Accenture's subcontractors for the purposes of administering the NHSmail services. This access takes place both within and outside the EU. Access outside the EU is governed through the use of EU Model Clauses in the relevant contracts.

Users may have this information updated either through self-service using the NHSmail Portal or by contacting their organisation's Local Administrator.

When a user leaves an organisation, their employing organisation should mark their account as a 'leaver'. It will then be removed from the NHS Directory after a period of time; it will still be visible to their organisation's Local Administrator within the NHSmail Portal.

This information is stored by Accenture within the UK. Some elements of the NHS Directory are also stored by Microsoft within Azure Active Directory.

Email, Skype and other collaboration data

Users of the NHSmail Live Service will create, store and send data through NHSmail. This could be through:

- Email (Exchange / Outlook).
- Instant Messaging, Voice, Video or Screen Sharing (Skype for Business).
- Office 365 services (SharePoint, OneDrive, Team, Yammer, etc.).

This data is controlled by the local organisations (Joint Controllers) and may include personally identifiable data or medical data. Local organisations are responsible for ensuring the data their users exchange through NHSmail has appropriate legal and governance controls in place, including putting Data Privacy Impact Assessments (DPIAs) in place and publishing appropriate privacy information to patients where relevant. For example, if a local organisation chooses to exchange medical data with a third party using an Internet based email service via NHSmail email, the local organisation would need to make sure that sharing was compliant with any applicable legislation, for example by notifying patients that this was occurring.

When a user leaves an organisation, their employing organisation should mark their account as a 'leaver'. This will then trigger the removal of their mailbox and associated content after a period of time. Data may be retained for up to two years after this point, for audit and compliance purposes.

This data may also be accessed by NSS, NHS Digital, Accenture and Accenture's subcontractors for the purposes of administering the NHSmail services including ensuring the security of the platform through preventing abuse of accounts or the transmission of malicious content or auditing of users' actions. This access takes place both within and outside the EU. Access outside the EU is governed through the use of EU Model Clauses in the relevant contracts.

Exchange and Skype for Business data are stored by Accenture within the UK. Office 365 data is stored by Microsoft, depending on the specific service this may either be within the UK, EU or outside the EU. For further information see Microsoft's privacy information.

Support tickets

Users of NHSmail may raise support tickets or requests with Accenture, for example when requesting to reset a password. This would normally include a user's name, contact details i.e. email, telephone, etc. and details of any issue they are experiencing and is normally exchanged over email or telephone.

This data may be accessed by NSS, NHS Digital, Accenture and Accenture's sub-contractors for the purposes of administering the NHSmail service. This data including support ticket records and any recordings of telephone calls is stored outside the EU. This is governed through the use of EU Model Clauses in the relevant contracts. This data is only to be used for the purpose of administering the services, it is not passed on to any third parties for marketing or any other purposes.

Other processing

The NHSmail Live Service deploys highly sophisticated SPAM and Malware filtering technologies to block SPAM, Viruses and Malware.

The NHSmail Live Service also runs the NHS Relay which is an insecure network for the routing of NHS email traffic that has not been deemed by local organisations (Controllers) initiating the email traffic, to require encryption.

The self-service password reset facility may contain personal mobile phone numbers supplied direct by users.

The NHSmail Live Service does not, itself, retain copies of or archives of emails and should not be considered an information storage or archiving solution. Service using organisations are responsible for providing archiving and back-up solutions for mailboxes they control.

The NHSmail Live Service retains audit logs about individual users and their access to the service. This is described in the Data Retention Policy.

Users calling the NHSmail helpdesk should note that all calls are recorded and stored for two months for quality purposes.

Extranet

The NHSmail Live Service Portal help pages are held on an extranet at: https://portal.nhs.net/Help/. This extranet uses essential cookies strictly for the purposes of providing web-based services. Cookie data used by Accenture (Processor) or their sub-contractors (approved by NSS) are not shared with other organisations and are used solely for the delivery of the Portal help pages. No consent for cookie use is requested as cookies are essential for the running of the site and are not shared with other parties. Without the use of these cookies, the function and usage of the extranet will be significantly impacted.

A cookie policy is available on our Portal help pages, providing details of the cookies collected, how they are stored and how they are used to deliver the Portal help pages.

Account registration

The NHSmail Live Service processes a wider selection of data as part of new applications for accounts from third party organisations, health and care organisations (such as pharmacy, optometry, dentistry and social care) including names and organisation details.

The NHSmail Live Service provides portal registration tools (web based) to allow users to register for NHSmail accounts. The portal registration tools support the setup of NHSmail accounts for health and care organisations (including pharmacy, dentistry, optometry, social care, locums). Data is collected to set up the new accounts and to support the authentication of users that access these portal sites.

Data used for authentication is stored for account maintenance purposes, such as password reset authentication, for the lifetime of the account.

This DPIA contains a record of the types of data that are used for data authentication.

3.5 Data Processing Guidance

The NHSmail Live Service (NSS, NHS Digital – Joint Controller) provides guidance and policy documentation on the running and maintenance of the service to inform local organisations (Joint Controllers) and their users.

Local organisations (Joint Controllers) are responsible for setting policies and procedures to govern the types of data that can be shared, with whom, with which countries / organisations and the ways in which NHSmail users send and receive data from other organisations / individuals / countries.

The NHSmail Live Service has provided some new guidance and policy information to support local organisations (Joint Controllers) with the completion of GDPR documentation including:

- NSS (NHSmail Live Service) Transparency Information.
- NHSmail Service: Joint Controller Arrangements

.

For NHSmail policy documentation and guidance visit the NHSmail Portal help pages.

4. Audience

This DPIA will be used by:

- NSS - as Joint Controller for the NHSmail Live Service.
- Accenture - as Processor for the NHSmail Live Service.
- Local organisations - as Joint Controller for the NHSmail Live Service.
- NHSmail end users.
- Public and patients.

This document illustrates the “privacy by design” approach taken in the development and maintenance of the NHSmail Live Service. The description and explanations it contains can be used by local organisations to form the basis for the completion of their Digital Transparency / Fair Processing Notice (privacy notices) that they as Joint Controllers (for the data they control locally) will need to provide.

NSS

This DPIA sets out the data that is processed and the justification for the legal and fair processing of this data by the NHSmail Live Service.

Live Service Board (NSS) provides governance and assurance over the running of the NHSmail Live Service.

Technical Design Authority (TDA) group reviews features and functionality changes proposed for the NHSmail Live Service to ensure they are technically viable, with additional responsibility to ensure data processing remains GDPR compliant.

A separate DPIA is in place for the NSS NHSmail service (as a user organisation of the NHSmail service, rather than the NHSmail provider role described in this DPIA).

Health and care organisations

This DPIA will be published as a public document to support local organisations (Joint Controllers) with the completion of their local documentation and guidance for their local GDPR compliance.

Information Governance staff, working for local organisations that use NHSmail, can use this DPIA and the wider guidance and policy documents held on the NHSmail Portal help pages to support the completion of local Transparency Information, guidance and GDPR compliance documentation.

Public and patients

NHSmail Live Service guidance and documentation is publicly available providing transparency of data processing and the way in which the service is managed and maintained.

5. Data Protection Impact Assessment Questions

5.1 Name of Stakeholder Group, Date Consulted and How Consulted

The NHSmail Live Service has been designed in context with the Data Protection Act with reviews held in recent years to ensure processing and guidance is uplifted to reflect the new GDPR legislation – Data Protection Act (DPA) 25 May 2018.

Stakeholder groups

- NHSmail Board.
- Local Administrators.
- All NHSmail users.

Examples of consultations held

GDPR discussions held at NHSmail Boards during 2017.

GDPR workshops held in April 2018 to finalise preparations including: NHS Digital (working on behalf of NSS) cross-functional representatives and Accenture Delivery Partner cross-functional representatives.

Workshops held to finalise planning in April 2018:

- NSS/NHS Digital : 9 April 2018
- NHS Digital & Accenture workshop: 11 April 2018
- NHS Digital & Accenture workshop: 24 April 2018

Information disseminated to Local Administrators (LAs) (representing the NHS organisations using the service) via monthly LA webinars and bulletins. Copies of the information disseminated to the Local Administrators is available on the Communications section of the Portal help pages.

GDPR information, and links to updated guidance / policy documentation, displayed on the Portal help page carousel in May 2018.

Guidance to be issued to all users in May 2018 – advising of Acceptable Use Policy update and how NHSmail meets the GDPR legislation.

- All user communication – May 2018

5.2 Is there a clear legal basis for the processing (collection, analysis or disclosure) of personal data?

There is a clear legal basis for processing of personal and confidential data through the NHSmail Live Service in the new context of GDPR:

Health and Social Care mandate and direction

The NHSmail Live Service is provided by NSS (as Joint Controller) via a five-year contract with Accenture (Processor) with an end date of 31 March 2021. The terms and conditions set out in the contract, which have been uplifted in accordance with GDPR legislation, via Variation Notice 12, stipulate that data must be processed in accordance with:

- Data Protection Act (1998).
- UK Data Protection Bill (14 Sep 17).
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
- Working Party 29 guidelines determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, wp248rev.01.

- Data Protection Act (2018).

Legal Considerations

The legal basis for processing, collecting, sharing and analysing data is the Direction issued by the Scottish Government eHealth Directorate where NSS is appointed as the Service Provider for NHSmail, taking responsibility for setting up and managing the data processing contract for the service on behalf of all Controllers.

NSS (Joint Controller) appointed Accenture as Processor via a commercial contract with an end date of 31 March 2021.

Additionally, the NHSmail Live Service requires individuals to agree to their personal data being managed by the NHSmail Live Service by accepting the Acceptable Use Policy (AUP) when their account is first initiated.

Legal areas that apply – NSS

The NHSmail Live Service (as Joint Controller) collects, shares and processes data within the NHSmail Live Service on the basis of Article 9 (2) (h) and Article 6 (b and e):

GDPR Article 9: Processing of special categories of personal data

Extract:

Article 9 (2) (h) – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Processing:

The NHSmail Live Service establishes email accounts in accordance with the staff details / data provided by local organisations (Controllers), or the individuals themselves, in accordance with Article 9 (2) (a) and (h).

The NHSmail Live Service processes patient and confidential information included in secure emails initiated by local organisations (Controllers) for processing by NSS, NHS Digital (Processor) and Accenture (Sub Processor) where the data is shared and processed in accordance with Article 9 (2) (h).

GDPR Article 6: Lawful Processing

Lawful processing by Controller (Article 6 (b and e);

(b) as part of their employment contract it is necessary for their job

(e) as the mail system is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Legal Areas that may apply – local organisations

Under GDPR legislation local organisations using NHSmail are additionally required to confirm their legal basis for using NHSmail within a locally held Transparency Information document (also known as Fair Processing Notice) for use by their employees.

The legal basis for local organisations (as the Joint Controller) to share and process data may be:

1. *Article 9 (2) (h) – processing is necessary for the purposes of preventive or occupational medicine.*
2. Lawful processing by Controller (Article 6 (b and e);

(b) as part of their employment contract it is necessary for their job

(e) as the mail system is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. <Public Task>

Local organisations should consider the legal basis that applies to them.

5.3 Are individuals clear about ways in which personal data about them is being used?

Policies, Guidance and AUP

The NHSmail Live Service has an Acceptable Use Policy (AUP) which staff are required to accept before using NHSmail. The AUP sets out the way the service runs, how users are expected to behave and the data retention periods for data stored about them and the data that they send and receive via the NHSmail service.

Policy documentation and guidance is available publicly on the NHSmail Portal help pages setting out how data is collected:

- Information Management Policy
- Access Policy
- Access to Data Policy
- Acceptable Use Policy (AUP)
- Data Retention Policy
- NSS (NHSmail Live Service) Transparency Information
- NHSmail Service: Joint Controller Arrangements

Joint Controller Responsibilities

NHS Digital provides policies and guidance to support local organisations (Joint Controllers) and NHSmail users with their use and compliance with the NHSmail Live Service terms and conditions:

- Acceptable Use Policy (AUP): states that individuals are responsible for reading these documents – all are required to agree before NHSmail account access is granted.
- Welcome Letter: issued when NHSmail account is first setup. Includes links to Portal help pages, training and guidance materials.
- Transparency Information: advises NHSmail users how their data is captured, used and stored and supports local organisations with the completion of Transparency Information notices for their organisation in accordance with their local policies and procedures.
- Joint Controller Arrangements: sets out the roles and responsibilities of the Controllers.
- All user comms: issued at least annually and provide links to Portal help pages.

Local organisations (Joint Controllers) are responsible for ensuring individuals have:

- Accepted and understand the AUP.
- Read and understood the policy documents and guidance published by the NHSmail Live Service on the Portal help pages https://portal.nhs.net/Help/, including the new Transparency Information.

NSS (as Joint Controller) will issue an all user email to NHSmail users in May 2018, including links to the new Transparency Information.

Federation with Partner Organisations

- Federation Partnership Agreements (FPAs) are documents with third party organisations, to agree access and use of the NHSmail Live Service platform specifically for Skype and Calendar services. Separate agreements are signed with each organisation wishing to federate accepting their responsibilities.

- Data may be provided to other partner organisations governed by the federation partnership agreement.

- Details of organisations that are federated are recorded on the NHSmail Portal help pages.

Local organisations (Joint Controllers) are required to use the Federation Partnership Agreements to inform their local security policies and procedures, which advise their staff which external organisations are suitable for secure collaboration.

Transparency Information

A new document has been produced to confirm how the NHSmail Live Service meets the GDPR duty of transparency and is called: NSS (NHSmail Live Service) Transparency Information.

Local organisations using NHSmail are required to ensure their staff have read and understood the policy documents and guidance provided by the NHSmail Live Service. The Transparency Information sets out how the NHSmail Live Service complies with GDPR and should be used by NHSmail users in conjunction with the Transparency Information provided by their local organisations (as Joint Controllers).

5.4 Is it necessary to collect and process all data items?

For each of the data categories below the justification for collecting, sharing and processing data falls into two core reasons:

- NHSmail Live Service – account setup.
- NHSmail Live Service – as secure email service (for processing of patient and sensitive data of NHSmail as their secure email service).

The following data categories are used by NSS (Joint Controllers), local organisations (Joint Controllers) and Accenture (Processor) to setup and manage NHSmail email accounts and collaboration tools provided by the NHSmail Live Service.

Data Categories [*Information relating to the individual*]	**Yes**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	Yes		NHSmail Live Service – account setup
Address	Yes		NHSmail Live Service – account setup - Work Address
Postcode	Yes		NHSmail Live Service – account setup - Work Address
Email address	Yes		NHSmail Live Service – account setup - Personal email address as Data Authentication prior to account provision - NHSmail email account stored on NHS Directory
			-

Data Categories [*Information relating to the individual*]	**Yes**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Mobile phone / device no.	Yes		NHSmail Live Service – account setup - Personal email address as Data Authentication prior to account provision - Work contact number stored on NHS Directory
Sensitive Personal Data			
Education / professional training	Yes		NHSmail Live Service – account setup - Work role / directorate stored on NHS Directory

NHSmail Live Service – as secure email service

NHSmail Live Service is used by local organisations (Joint Controller) and their users to securely send and receive sensitive or official data (including patient identifiable data).

The following data categories may be included by local organisations (Joint Controllers) within emails or collaboration tools provided by the NHSmail Live Service for processing by Accenture (Processor) to other recipients as directed by the end users and local organisations (Joint Controllers).

Data Categories [*Information relating to the individual*]	**Yes**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	Yes		NHSmail Live Service – as secure email service
Address	Yes		NHSmail Live Service – as secure email service
Postcode	Yes		NHSmail Live Service – as secure email service
Date of birth	Yes		NHSmail Live Service – as secure email service
Marital status	Yes		NHSmail Live Service – as secure email service
Gender	Yes		NHSmail Live Service – as secure email service
Email address	Yes		NHSmail Live Service – as secure email service
Physical description	Yes		NHSmail Live Service – as secure email service
Home phone number	Yes		NHSmail Live Service – as secure email service
Mobile phone / device no.	Yes		NHSmail Live Service – as secure email service
Sensitive Personal Data			

5.5 Will personal data be shared and/or merged with other datasets?

Personal Staff Data

Data about staff is stored against their NHSmail account including name, telephone number, job

role. This data is visible to the NHSmail user via the NHSmail Portal and can be updated and changed by the user as required.

Local organisations may use the Connector service (TANsync) to maintain staff details which will match / combine data supplied by the local organisation. Data sets (matched or unmatched) may be exchanged by email but the NHSmail service itself will not match or combine these items.

Local organisations and staff are required to review and maintain personal data stored within the NHSmail Live Service

GDPR definition : Personal Data

Official Data

NHSmail is used by local organisations to send / receive data including patient / service user / client identifiable data and related health and social care data. Includes sensitive data.

Organisations use the NHSmail Live Service in line with their local policies and procedures which could involve this class of data. For example, sending patients appointment reminders, archiving emails according to local data storage procedures.

NHSmail supports open APIs, allowing organisations to programmatically send / receive secure data to / from other systems (such as e-referral systems).

Local organisations using APIs to extract data personal or official data from the NHSmail Live Service are required to protect and secure this data via their local processing standards and policies. Once data is extracted, the local organisation becomes the Controller for this data.

GDPR definition: Special Category Data

5.6 How long will personal data be retained?

Personal Staff Data
Data about staff is stored for as long as the account is active.

NHSmail Email Data

The NHSmail Data Retention Policy sets out data storage periods for the service.

Centrally. copies of email sent / received are retained for 180 days for forensic audit purposes and message summaries for two years.

Organisations use the NHSmail Live Service in line with their local policies and procedures which could involve storage of data locally for more than two years.

Leaver Policy

NHSmail accounts transfer between organisations using the Leaver Policy, allowing individuals to keep the same email account throughout their career.

Local organisations (Joint Controller) are required to set guidance for staff that leave their organisation to retrieve any relevant data that is held within the NHSmail user account prior to their departure. This data will also be stored centrally, as described above, in accordance with the Data Retention Policy.

Forensic requests for staff that have left can still be submitted by local organisations (Joint Controllers) for the periods of employment that apply.

NHS Directory

The NHS Directory information is retained for as long as the account is active.

Local organisations (Joint Controller) responsible for maintaining / deleting contact details held on the NHSmail Directory – known as NHS Directory.

Other

The service retains audit logs about individual users and their access to the service. These are described in the Data Retention Policy.

Users calling the NHSmail helpdesk should note that all calls are recorded and stored for two months for quality purposes.

5.7 How will standards of data quality be achieved and maintained?

Personal Data

Personal data can be edited by the local organisations (Joint Controller) to ensure records are kept current.

NHS Directory and NHSmail Portal

This is maintained by the administrators in the local organisation employing the member of staff, it may be maintained either through the NHSmail Portal or through an automated synchronisation from a local directory (i.e. with TANSync). For certain fields (i.e. telephone number) the user can update these themselves through self-service.

Email, Skype and other collaboration data

Data quality for content sent over email or Skype or stored within other collaboration tools is the responsibility of the user sending / uploading the information. In the event it is incorrect the user should update and re-send / upload the corrected information.

5.8 Are individuals made aware of their appropriate rights (under certain circumstances)?

NHS Opt-out – How has it been considered?

Not applicable as NHS Opt-out refers to patients only and the processing carried out by NHSmail does not relate to the use of patient data for secondary purposes.

GDPR Rights – How have these been considered?

The rights available to individuals in respect of the NHSmail Live Service and Data Exchange processing.

NHSmail Live Service	**Data exchanged using NHSmail**
The Live Service relies upon the legal basis of "legal obligation" for processing personal data i.e. the processing is necessary for compliance with a legal obligation to which the Controller is subject. Applicable rights are: • Right to be informed • Right of access • Right to rectification • Right to restrict processing – where an individual contests the accuracy of the personal data, processing should be restricted until accuracy has been verified	The appropriate legal basis for processing personal data for the purpose of using the NHSmail service must be identified by local organisations. If the appropriate legal basis for processing personal data and special category personal data (sensitive personal data) is "public task" (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller) then applicable rights are: • Right to be informed

These rights are described in the Transparency Information. Rights which do **not** apply to processing carried out on the legal basis of "legal obligation are: • The right to erasure • The right to data portability • The right to object • Rights in relation to automated decision making and profiling	• Right of access • Right to rectification • Right to restrict processing – where an individual has objected to the processing and the Controller must consider whether the Controller's legitimate grounds override those of the individual • Right to object (based on grounds relating to his or her particular situation) – unless the Controller can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims • Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (unless processing is necessary for reasons of substantial public interest)

	NHSmail Live Service	Data exchanged using NHSmail
The right to rectification:	Email account set-up errors can be corrected by NHSmail Local / Global Administrators.	Email account set-up errors can be corrected by NHSmail Local / Global Administrators. NHS Directory errors can be corrected by the individual or their Local Administrator. If TANSync or a connector is used for managing Directory data, Local Administrators have this responsibility.
The right to erasure:	When processing based on a legal obligation, the individual has no right to erasure, right to data portability, or right to object.	Data is kept for the duration of the Data Retention Policy after which, it is permanently deleted. In exceptional circumstances, users may be 'hidden' from the NHS Directory although data will be maintained as per the Data Retention Policy.

.

5.9 If individuals exercise their rights how are these rights upheld?

Local user organisations (Joint Controllers) are responsible for providing Transparency Information to those affetced by the processing and having procedures in place to ensure the rights provided by the appropriate legal basis can be exercised.

The NHSmail Live Service, on the legal basis of “legal obligation”, upholds the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to restrict processing

In addition, individuals who are not satisfied with the response from the NHSmail Live Service or believe their data is not being processed in accordance with the law, can complain to the Information Commissioner’s Office (ICO) which is the regulator for Data Protection and upholds information rights. More information is available on the ICO website https://ico.org.uk/.

How individuals can exercise these rights is described in the Transparency Information provided to all users.

Process Summary

Rights	How upheld by NHSmail Live Service	Local organisation responsibilities
Right to be informed	NSS: NHSmail Live Service Transparency Information advises NHSmail users how their data is captured, used and stored and supports local organisations with the completion of Transparency Information notices for their organisation in accordance with their local policies and procedures	Transparency Information must be provided to NHSmail users setting out how local policies and procedures apply to the capture, use and storage of their data.
Right of access	Due to the high volumes of data processed on the NHSmail service, and the central storage of this data, this activity will be completed by th the Processor (Accenture).	Requests should be made to the NHSmail Local Administrator within the health and care organisation that owns your NHSmail account (normally your employer).
Right to rectification	If the NHSmail Live Service has recorded your personal details within the service, including the NHS Directory, incorrectly or it is incomplete, you can make a request to your NHSmail Local Administrator or the NHSmail helpdesk who can make the necessary amendments. Guidance on finding your Local Administrator is available.	Local Administrators are responsible for supporting NHSmail users to make the necessary amendments. Guidance on finding your Local Administrator is available.
Right to restrict processing – where an individual contests the accuracy of the personal data, processing should be restricted until accuracy has been verified	A condition of using NHSmail is that the NHS Directory is populated with user information as it is not possible to operate the service without it.	Requests should be made to the NHSmail Local Administrator within the health and care organisation that owns your NHSmail account (normally your employer).

Requests for an NHSmail account to be removed are processed by the Local Administrators,

National Administration Service (Accenture) or the National helpdesk (Accenture), using the standard leavers' process. Requests from individuals to be immediately deleted (forgotten) will be considered in accordance with Article 17 GDPR subject to authorisation from the local organisation (Joint Controller) where the individual was employed.

Requests for hiding an individual from the NHS Directory require permissions from the owner or HR director to be forwarded to the NHSmail Live Service Operations Team (NSS) via nhsmail.scotland@nhs.net before the NHSmail helpdesk (Accenture) can action. Urgent requests can be processed by logging the information with the NHSmail Operations Team while raising a service request in parallel.

5.10 Have technical and organisational controls for "information security" been considered?

The NHSmail Live Service is accredited to the NHS secure email standard and is compliant with ISO27001 and a number of security standards.

Accreditation	Certificate Number
ISO 9001:2015	FS 571552
ISO/IEC 20000-1:2011	ITMS 535634
ISO/IEC 20000-1:2011	ITMS 571355
ISO 22301:2012	BCMS 523309
ISO 22301:2012	BCMS 556058
ISO/IEC 27001:2013	IS 589293

These certificates can be viewed via the BSI validation tool:

The NHSmail Live Service is audited on an annual basis (IT Health Check or Pen Test) by an independent organisation to ensure security standards and service levels are maintained at the highest possible levels.

A System Level Security Policy (SLSP) is in place between NHS Digital/NSS (Joint Controller) and Accenture (Processor) which captures the system infrastructure and security protocols in place for the NHSmail Live Service. This is a commercially sensitive document which cannot be shared. NHS Digital/NSS, as Joint Controllers, manage the SLSP on behalf of local organisations (Joint Controllers).

The NHSmail helpdesk and service management for the NHSmail Live Service operate in accordance with the ITIL service management framework. Accenture are fully compliant with the ISO20000-1:2011 Service Management System (SMS) standard and are annually re-accredited to confirm continued compliance by an independent business standards organisation (BSI).

The NHSmail Live Service Technical Design Authority (TDA) has responsibility for overseeing design changes and proposed developments to the service. The TDA ensures all changes are:

- Secure by design and maintain accreditation to the secure email standard.
- Maintain the integrity of the Core Service design as contracted.
- Align to Information Governance Standards.
- Align to accreditation certificates (as listed above).

TDA recommended changes are approved by the NHSmail Board (chaired by NHSmail Product Owner) and are implemented by Request for Change (RFC) notices.

Contractual

A GDPR Compliant Contract is in place between NSS (Joint Controller) and Accenture (Processor). The NHSmail Live Service contract includes Service Level Agreements (SLAs) which Accenture (Processor) are required to uphold. The NHSmail Live Service contract, and these SLAs, are managed by NHS Digital/NSS (Joint Controller) on behalf of all Controllers. The SLA status is published on the NHSmail Portal help pages.

Information Governance

Local organisation (Joint Controllers) are required comply with the Scottish Information Governance Framework and to ensure that NHSmail users have completed IG training. New organisations joining NHSmail are required to self-declare IG compliance before NHSmail accounts are authorised.

Local organisations (Joint Controllers) appoint Local Administrators (LAs) to manage and maintain the NHSmail service for their organisation including the adding, removal and suspension of NHSmail accounts. Local Administrator guidance is provided via the NHSmail Portal help pages, monthly webinars and bulletins.

OR

Local organisations (Joint Controllers) are required to appoint shared mailbox owners (privacy officers) to oversee the IG and data management for their site. These arrangements are typically for smaller organisations that:

- Appoint a Local Sponsoring Organisation (e.g. Health Board) to provide the administration and maintenance of the email accounts and collaboration tools.

Shared mailbox guidance is provided via the NHSmail Portal help pages (available at : https://portal.nhs.net/Help/), and user group specific bulletins.

System Security

The NHSmail service includes a number of security features intended to prevent the transmission and storage of spam or malware through the platform. It also includes various security monitoring technologies to detect attacks or abuse of the system.

5.11 Will personal data be transferred outside the EEA?

This section describes the way in which the NHSmail Live Service uses and stores personal data.

Local organisations (Joint Controllers) have a responsibility to include these details, and any local arrangements that affect the way in which NHSmail data is stored or accessed, in their local Transparency Information document (Fair Processing Notice).

Cloud Act

It is noted that (in common to a degree with the refinement and understanding of the GDPR legislative requirements in practice), the US Clarifying Lawful Overseas Use of Data Act introduces uncertainty on NHSmail Live Service obligations in respect to any future requests for the disclosure of data.

It is not clear, nor is there any established precedent, on the implications for NSS as a Joint Controller should this occur, and this lack of clarity means there is an open risk with regards to this matter.

NHS Directory & NHSmail Portal

The NHS Directory (directory within the NHSmail system) and the NHSmail Portal (known as the Portal) contains data that can be accessed by any health and care member of staff with an active NHSmail account.

This data may also be accessed by NSS, NHS Digital, Accenture and Accenture's subcontractors (as approved by NSS) for the purposes of system design, security and general administering of the NHSmail Live Service. Access to the NHS Directory and Portal takes place both within and outside the EU. Access outside the EU is governed through the use of EU Model Clauses in the contract with NSS and the relevant subcontractor contracts.

Some elements of the NHS Directory are also stored by Microsoft within Azure Active Directory which is stored within the EU and United States – for further information see Microsoft's privacy information.

Email, Skype and other collaboration data

This data may be accessed by NSS, NHS Digital, Accenture and Accenture's subcontractors for the purposes of administering the NHSmail Live Service including ensuring the security of the platform through preventing abuse of accounts or the transmission of malicious content or auditing of users' actions. This access takes place both within and outside the EU. Access outside the EU is governed through the use of EU Model Clauses in the contract with NSS and the relevant subcontractor contracts.

Exchange and Skype for Business data is stored by Accenture within the UK. Office 365 data is stored by Microsoft, depending on the specific service this may either be within the UK, EU or outside the EU and may be dependent on a local organisation's (Joint Controller) arrangements with Microsoft. For further information see Microsoft's privacy information.

Support tickets

Users of NHSmail may raise support tickets or requests with Accenture, for example when requesting to reset a password. This would normally include a user's name, contact details (i.e. email, telephone, etc.) and details of any issue they are experiencing and is normally exchanged over email or telephone.

This data may be accessed by NSS, NHS Digital, Accenture and Accenture's subcontractors for the purposes of administering the NHSmail Live Service. This data, including support ticket records and any recordings of telephone calls, is stored outside the EU. This is governed through the use of EU Model Clauses in the relevant contracts.

6. Further Actions

Completed DPIAs must be revisited during the lifecycle of the project / programme / service, to ensure:

- Outcomes and measures identified are still relevant.
- Actions recommended to mitigate risks are implemented.
- Mitigating actions are successful.
- Upload the approved DPIA to the Unified Register.

Action	Date	Owner
Uplift after DPA 2018	25 May 2018	NHSmail Product Owner
Consult with NHSmail users and wider stakeholders to consider refinement or areas for clarification	August 2018	NHSmail Product Owner
Review and uplift prior to O365 Hybrid implementation	September 2018	NHSmail Product Owner

Planned reviews:

Date	Reason	Owner
May 2018	GDPR Uplift	NHSmail Product Owner
September 2018	O365 Hybrid Launch	NHSmail Product Owner
April 2019 (and yearly thereafter)	Annual Review	NHSmail Product Owner
January 2021	Planned activities for contract closure	NHSmail Product Owner