NHSmail: Access to Data Procedure

Facilitating access to email data for organisations consuming NHSmail

March 2021
Version 6

Contents

Introduction

When dealing with some official investigations, NHS trusts, boards or other authorities will require access to NHSmail email data held in the name of one or more of their employees. These requests typically fall into two categories:

1. Human Resources (HR) disciplinary investigations, investigations by or on behalf of the police or the NHS Counter Fraud Service or other bodies such as these.
2. Data Subject Access Requests (DSARs) - Individuals have the right to access their personal data under data protection legislation.

Both such categories are referred to throughout this document as 'investigation requests'.

If organisations are unable to fulfil the request locally, a request can be submitted to the NHSmail live service team or National Services Scotland (NSS), dependant on locality.

Purpose of document

This document covers the procedural approach to facilitate access to NHSmail data on behalf of NHSmail consuming organisations.

It will ensure data requirements are duly authorised and that disclosure is made only to the appropriate organisations and in the appropriate manner.

This document does not cover how data will be processed. This is the responsibility of the local consuming organisation requesting access to NHSmail data.

Submitting an investigation request

The NHSmail live service team or National Services Scotland (NSS) will only accept investigation requests submitted from the Local Administrator of the NHSmail consuming organisation i.e. the organisation that administers the NHSmail account(s) in question and must adhere to the guidance in this document.

The NHSmail live service team or National Services Scotland (NSS) will require the investigation request to be approved as outlined below.

Organisation Type	Authorised Approver

NHS trust, health board or NHS England local area team	Chief executive or HR director or equivalent role in an NHS trust or health board
Commissioning Support Unit	Managing director
Clinical Commissioning Group (and the GP practices in its designated geographical area)	Accountable officer
GP locums (England only)	NHS England responsible officer
Pharmacy, dentistry and social care managed by the National Administration Service (NAS)	England - shared mailbox owner Scotland - Chief executive or HR director or equivalent role in a health board

The requesting organisation must take ownership of the data that is received from the NHSmail live service team or NSS as a result of their request and provide an NHSmail email address (@nhs.net) for the data to be sent to.

Once the output from the forensic discovery request has been fulfilled and sent to the recipient, responsibility and ownership of the data is transferred to the receiving organisation and the chain of custody is considered as complete. For the avoidance of doubt, Accenture or NHS Digital are not responsible for the data once it has been sent to the receiving organisation. On receipt of the data, the organisation must ensure it is stored securely and managed in accordance with local information governance policy and data protection legislation.

All requests must be submitted by a local administrator (LA) via the online form obtained from Helpdesk Self-Service.

The LA must be logged into their NHSmail account to access Helpdesk Self-Service and guidance on completing the form is available in the article forensic discovery requests.

Upon completing the online form, please ensure approval evidence from the Authorised Approver (as outlined in the table above) has been attached.

Note: the information requested via Helpdesk Self-Service is the same as was previously submitted to feedback@nhs.net and nss.nhsmailscotland@nhs.scot via an embedded form within an email, utilising Helpdesk Self-Service provides a fully auditable request following the standard helpdesk processes

The following types of information can be provided to the requesting organisation:

- **Journal 180-day full email message content:**
    - For a stated NHSmail mail account.
    - The 180-day period begins from when the service provider instigates the request.
    - This includes the full email message, including any email attachments and any Skype for business conversation history.

- It does not include screen shares, presentations in meetings or voice or video using Skype for Business.

Journal 24 months of email summary data:

- This includes the meta data only (to, from, subject, time / date) and is provided in a Microsoft Excel spreadsheet format.

Mailbox snapshot

- This can be provided to allow the requestor a full copy of the user's mailbox at the time of the request being processed. This type of request is supported where an organisation needs to ensure they have full capture of all available data within a user's account.

- It is not possible to request the 'Journal 180-day full email message content' information for email accounts that have been converted into an 'application' account. It is still possible however to request 24 months of summary data for these high- volume sending accounts.

- A mailbox snapshot is a replica of a user's mailbox at the time of the search and therefore may contain historic sensitive information. For example, emails relating to previous organisations the user may have worked for if they have not followed the leaver/joiner guidance to delete role specific emails when transferring organisations. It will also not contain any permanently deleted emails which are older than 180 days.

As part of an official investigation, data within the retention period of 180 days (since last edited) can be accessed for the following Office 365 applications (for those organisations using NHSmail Office 365 Hybrid):

- OneDrive for Business accounts
- SharePoint site collections
- Office 365 groups (including emails to groups, conversation and files transferred in Teams channels conversation and file transfer)
- Teams private (one-to-one) conversation (IM only)
- Yammer

The NHSmail live service product owner or NSS equivalent, or nominated deputy, will be sent your request to check and approve.

Issuing an investigation request

Once a request has been approved the NHSmail live service team / NSS will pass the request to the service provider for retrieval of the data.

The NHSmail live service team / NSS and the service provider will handle all requests on a 'first come, first served' basis and, depending on the number of requests being processed, can take up to 10 working days. If your request is urgent due to a statutory deadline, please state this on your request. Every effort will be made to prioritise urgent requests.

Once the service provider has completed the investigation, the information will be provided to the user of the requesting organisation noted on the form in one of the following methods.

Note: The method of how the data is presented will depend on the type of Forensic Discovery chosen and whether the mailbox data resides on the existing NHSmail On-Premise platform or, the new Microsoft Exchange Online platform.

	Types of information	**Output Format**	**Folder Structure Retained**
Exchange On-Premise	Journal 180-day full email message content	pst file	No
	Journal 24 months of email summary data	Microsoft excel	No
	Mailbox snapshot	.pst file	Yes

	Types of information	**Output Format**	**Folder Structure Retained**
Exchange Online	Journal 180-day full email message content	.pst file	Yes
	Journal 24 months of email summary data	Microsoft excel	No
	Mailbox snapshot	.pst file	Yes

Note:

- Under no circumstances will investigation material be sent via internal or external postal services or in any ‘hard copy’ format.
- Neither the NHSmail live service team / NSS or the service provider will attempt any data analysis on the investigation results. Any data manipulation or filtering is the requesting organisation’s responsibility.

Requesting organisations must take steps to ensure that the information being returned in the investigation is handled appropriately in accordance with data protection legislation. In particular, due to the sensitivity of the information within these requests it is the duty of the requesting organisation to ensure that employees who have access to the data have had the appropriate information governance and data protection training.

Please see below the steps you can follow to view the results for the Forensic Request:

- Click on the link and download the Files (These files are zipped and PW protected, You will Require 7Zip to extract the files)
- Once downloaded, please extract the files locally and then copy the PST file to the final destination. Please be advised, these can be large PST files therefore extracting them across a network can be very slow and may fail. Please use local storage where possible to minimise the time required to transfer the PST file to the final destination.