Transferring data into NHSmail

February 2018
Version 2

Contents

Introduction

This guide sets out the risks associated with individuals or organisations transferring (copying) data from an existing email system (or archive tool) into NHSmail, or other health and care email systems.

Organisations are required to read and understand this guide, before commencing their migration to NHSmail. Organisations are advised to set up local guidance for their users, to support any on-going data transfer that may take place.

This guide is relevant for all:

- organisations self-migrating to NHSmail
- commissioned/independent providers joining NHSmail
- individuals moving data from local data sources into NHSmail
- anyone moving data from one system to another within health and care.

Data transfer into NHSmail

Pre-requisite steps

Organisations that are migrating to NHSmail must ensure that all computers and servers are patched to the latest recommended levels, before commencing their migration. A full hygiene check must also be completed by local IT teams across all mailboxes earmarked for transition. Information can be found on the NHS Digital website.

Further information is available by contacting the CareCERT team directly on carecert@nhsdigital.nhs.uk, or by calling 0800 0856653.

Confirmation needs to be provided to the NHSmail team via feedback@nhs.net, confirming steps have been completed, before migration, and the movement of data can commence. Additional checks may be enforced as part of a managed migration.

Transferring data

Before transferring data into NHSmail, organisations are required to carry out a full scan using the latest anti-virus software, as procured by your organisation, to avoid the inclusion of undesirable content including Malware. Data that is not scanned before transfer presents a risk to an organisation, as a user may inadvertently click on old links, causing harmful damage to other local systems and services.

The risk of transferring undesirable data content to other users within NHSmail, or other health and care systems, will be dependent on:

- the level of security applied locally within an organisation
- the level of understanding by end users of the risks associated with harmful data access and transfer
- the level of security in place on the target email platform.

To mitigate risks, the following steps must be undertaken:

- ahead of, and during, the scanning and data transfer process, where possible, organisations must take steps to protect NHSmail by isolating other local systems
- local guidance for end users must be developed and circulated, to ensure they understand:
    - the risks associated with data transfer
    - the steps to take to mitigate these risks
    - their responsibilities as custodians of data and information governance for the NHS
- since data transfer may be initiated by an end user at any time (not just at migration to a new system), regular security and IG training must be monitored and enforced locally for all mandatory training.

NHSmail utilises anti-virus and anti-spam protection, designed to isolate and remove harmful email links and threats that are transmitted through the platform. In addition, exchange mailbox searches are performed on a regular basis to actively remove any undesirable data from inboxes and folders stored on the NHSmail platform. These checks provide protection to the existing email users during, and after, a data transfer process is completed.

Summary of data transfer requirements

- Ensure all computers and servers are patched to the latest levels.
- Scan local email data and any PST files held locally, before commencing data transfer.
- Scan local archiving systems on a regular basis to ensure data integrity is maintained.
- Develop and circulate guidance to end users, to ensure local understanding of the risks of transferring data into the organisation’s email system.
- Provide written confirmation to the NHSmail team via feedback@nhs.net (or secure email provider) that patches are all updated and scans of data completed. This should be communicated by your NHSmail project manager, as part of the migration checklist process, once assurance and approval to proceed is confirmed by the CIO or IT director responsible for the NHSmail implementation locally.
- The data transfer preparation outlined in this document is mandatory for all organisations migrating to, or using a secure email system, such as NHSmail.