Encryption Guide for NHSmail

March 2018
Version 4

Contents

Introduction

Purpose of Document

Target Audience: All end users of NHSmail

The NHSmail service includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services, for example, nhs.uk (please note that *.secure.nhs.uk is considered secure), gmail, Hotmail. This document is designed for all end users of NHSmail and gives information on how and when to use the encryption feature.

Before using the encryption feature, please ensure you read and understand all guidance and instructions on using the feature to ensure data remains secure.

Once a message is sent from NHSmail, it is encrypted and protected with a digital signature to assure the recipient that the message is authentic and has not been forged or tampered with. Formatting of the message is preserved, and attachments can be included.

Note: please ensure your organisation is happy for you to communicate sensitive information to non-accredited or non-secure recipients using the NHSmail Trend Encryption Micro service and that you always adhere to local information governance (IG) policies.

When to use the NHSmail encryption feature

NHSmail users can exchange sensitive information securely with other NHSmail users, without needing to use the encryption feature. For example, sending from @nhs.net to @nhs.net.

If you are sending sensitive information outside of NHSmail, then the encryption feature should be used. The only exception is when sending to emails ending in *secure.nhs.uk

If there is doubt or uncertainty, you should use the NHSmail encryption feature. NHSmail will then encrypt the email only if the destination domain is not secure. If sending an email to multiple organisations with some secure and some insecure domains, those that are secure will receive an unencrypted email and those that are not secure will receive an encrypted email.

How to send an encrypted message

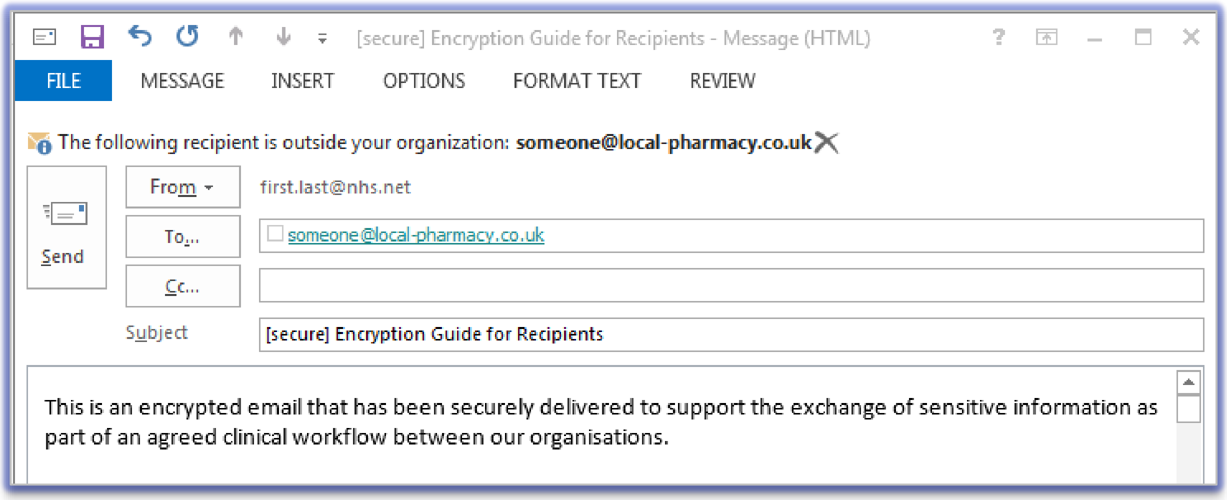
Before sending patient or sensitive data via the encryption service, it is good practice to set up the 'encrypted channel' which helps verify the correct recipient:

1. Send the recipient the accessing encrypted emails guide for non-NHSmail users, so they can register for the service.
2. Once the recipient of the information has registered for the encryption service and confirmed to the sender this is complete, patient and sensitive data can be sent within an email or as an attachment, subject to local governance policies.

3. Follow the steps below to send an initial encrypted email but **do not** include patient or sensitive information the first time. This is to 'set-up' the secure channel of communication and ensure the correct recipient has successfully received the email. If it is an incorrect recipient, data has not been compromised.

To send an encrypted email:

4. Log in to your NHSmail account (either via an email client such as Outlook or via the web portal at www.nhs.net).
5. Create a new email message in the normal way.
6. Ensure the recipient's email address is correct.
7. In the **subject** field of the email, enter the text [secure] before the subject of the message. The word secure **must** be surrounded by the square brackets for the message to be encrypted. If square brackets aren't used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment.
8. Type the message.



[secure] Encryption Guide for Recipients - Message (HTML)

The following recipient is outside your organization: **someone@local-pharmacy.co.uk**

From: first.last@nhs.net

To...: someone@local-pharmacy.co.uk

Cc...:

Subject: [secure] Encryption Guide for Recipients

This is an encrypted email that has been securely delivered to support the exchange of sensitive information as part of an agreed clinical workflow between our organisations.

9. Click on **send** to send the message. An unencrypted copy will be saved in your **sent items** folder.

Once the initial registration process has taken place, you can then send other emails with required attachments.

The service will then encrypt the message and deliver it to the intended recipient. The sent item will be stored unencrypted in your sent items folder, and any replies received will be decrypted and displayed as normal in NHSmail.

Note: [secure] is not case sensitive and [SECURE] or [Secure], for example, could also be used.

Keeping encrypted emails secure

Before sending an encrypted email, you should ensure that the recipient is expecting it and is ready to handle the contents appropriately either as part of an agreed clinical or sensitive business workflow, particularly if it contains sensitive or patient identifiable information.

Exchanging patient / sensitive information should be done in accordance with local information governance policy / procedures and the NHSmail acceptable use policy.

A number of attachment types are not permitted to be sent via NHSmail, these include .exe files. If a non-permitted attachment is detected it will automatically be removed. For the full list of non-permitted attachments see the attachments guide.

Note: it is your responsibility and legal duty under the Data Protection Act 1988, on behalf of your employing organisation, to safeguard any data received in line with the data protection and information governance requirements agreed between your organisation and the receiving organisation. If required, and in line with your local information management policies and processes, you should retain unencrypted copies of any encrypted email received in your local information repositories.

Help and further guidance

Call the national NHSmail helpdesk on 0333 200 1133 or email helpdesk@nhs.net.

Recipients of NHSmail encrypted emails who require help with registration, should refer to the accessing encrypted emails guide for non-NHSmail users.

Frequently asked questions

Where is the data processed?
Data is encrypted on the NHSmail platform within the United Kingdom. When a recipient of encrypted email authenticates to the service to open the encrypted content or uses the zero-based download reader (Trend Micro software used to access encrypted files), these actions are processed in the United Kingdom.

While being processed, the message is cached by the UK servers for up to an hour and then permanently erased after the hour elapses. Once encrypted, the reply is only unencrypted when it arrives on the NHSmail platform within the United Kingdom.

Does the encryption feature work when NHSmail is accessed on all browser types?
Yes. The encryption feature works when NHSmail is accessed from all recommended browser types. These are Internet Explorer 9 or above and latest versions of Chrome, Firefox and Safari.

Is message tracking (for example, delivery or read receipts) available on encrypted emails?
No.

Do I have to register for the service to decrypt replies?
No. Replies are received encrypted to the NHSmail service. Once received into the NHSmail data centre, the reply is decrypted and delivered to your inbox as though it was a normal email.

Can I set up an application linked to NHSmail which will send automated encrypted emails?
Yes, as long as the subject line contains the encryption keyword – [Secure] and the application is locally signed off for clinical use.

Can encrypted replies received by generic mailboxes be accessed as normal?
Yes.

What is the maximum attachment size I can send on encrypted email replies / forwards?
35mb.

What types of attachments can be included on encrypted email replies / forwards?
Certain file types are blocked by the NHSmail service and cannot be sent or received. The list of blocked attachments can be found in the attachments guide.

Is the service suitable for urgent, real-time communication?
As the service sends and receives email over the internet there are no guarantees that a message will reach its intended recipient as internet email can be silently lost, even when delivery reports are requested.

Equally, there is no guarantee on how quickly the message will be delivered or the availability of the service the recipient uses to process the message.

We would recommend organisations develop mitigations, through their local business processes, around loss of messages or being unable to open files.

Can the service be used to communicate with nhs.uk email addresses?
Yes. Organisations that run their own local email service can receive encrypted emails from NHSmail users and reply to them, avoiding the need for having both a local and NHSmail email account.