Encryption Guide for NHSmail

March 2021 Version 8.1

Contents

Introduction

This document is designed for all end users of NHSmail and gives information on how and when to use the encryption feature.

NHSmail includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services, for example Gmail, Hotmail etc.

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

Once a message is sent from NHSmail using the encryption feature, 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 has given approval for you to communicate sensitive information to non-accredited or non-secure recipients using the NHSmail encryption 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 emails to an organisation that has accredited to the secure email standard. A list of these accredited domains is available on NHS Digital's website.

If there is doubt or uncertainty you should use the NHSmail encryption feature, which will encrypt the email unless the recipient is an accredited domain.

If sending an email to multiple organisations with some secure and some insecure domains, using the encryption feature means that automatically 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 an encrypted email

Exchanging patient / sensitive information should be done in accordance with local information governance policies and the NHSmail Acceptable Use Policy.

Before sending patient or sensitive data via the encryption service 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
- Send the recipient the accessing encrypted emails guide for non-NHSmail users, so they can register for the service
- Send an encrypted email as a test following the instructions below, 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.

Once you have established the secure channel of communication, patient and sensitive data can be sent within an email or as an attachment, subject to local governance policies.

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

Note: It is your responsibility and legal duty under the Data Protection Act 2018, 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.

To send an encrypted email

1. Log in to your NHSmail account (either via an email client such as Outlook or via the web portal at www.nhs.net).
2. Create a new email message.
3. Ensure the recipient's email address is correct.

4. In the **Subject** field of the email, enter the text **[secure]** either before or after the subject of the message. The word secure **must** be surrounded by the square brackets for the message to be encrypted.
   Note: If square brackets are not used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment.
5. Type the message.

6. Click on **Send** to send the message. The service will then encrypt the message and deliver it to the intended recipient.
7. An unencrypted copy will be saved in your **Sent Items** folder.

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

Any replies received will be decrypted and displayed as normal in NHSmail with the orange Egress banner which includes details of when the email was decrypted, as per below.

From: "Joe Bloggs Test" <JoeBloggstest@gmail.com>
Sent: Thursday, February 20, 2020 2:47 PM
Received: Thursday, February 20, 2020 3:23 PM
To: Test <Test@nhs.net>
Subject: RE: [Secure] Results of blood test

This email, created by joebloggstest@nhs.net, has been securely delivered using Egress Switch and was decrypted on 20 February 2020 15:23:42+00:00

Hi Test

Thank you for your email, I can confirm I have received it and will book an appointment at the surgery. Thanks,

Joe Bloggs

Revoking access to an encrypted email

It is possible to revoke access to an encrypted email and attachment sent via Egress. This should only be used when there is a genuine reason why the email should no longer be able to be accessed or, for example, if it was sent in error.

You can look at details of every secure email that you have sent via the Egress Web Portal.

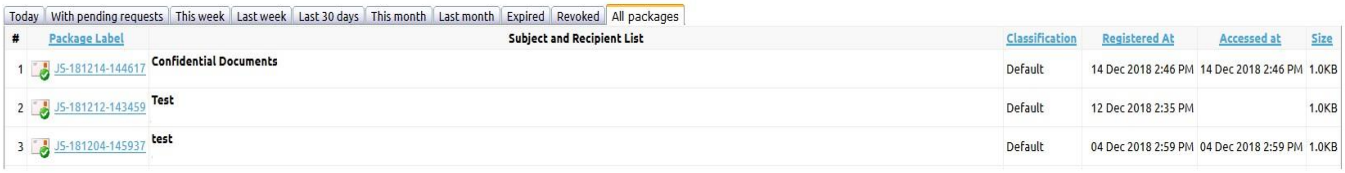
Note: This does not show you a copy or the contents of the secure email that was sent.

How to view your sent secure email

1. Log into the Egress Web Portal at https://esi.nhs.net

2. Select **Sent Packages** and then the tab that corresponds to the date you sent the email you are wanting to check or change permissions for.

3. Select the **Package Label** of the email you would like to see. This will open a new window.



Sent package options

Sent Packages displays a list of all secure emails that you have sent via the Egress Web Portal. This enables you to manage secure information in real-time meaning even after you have sent the email you have some control over the information by being able to:

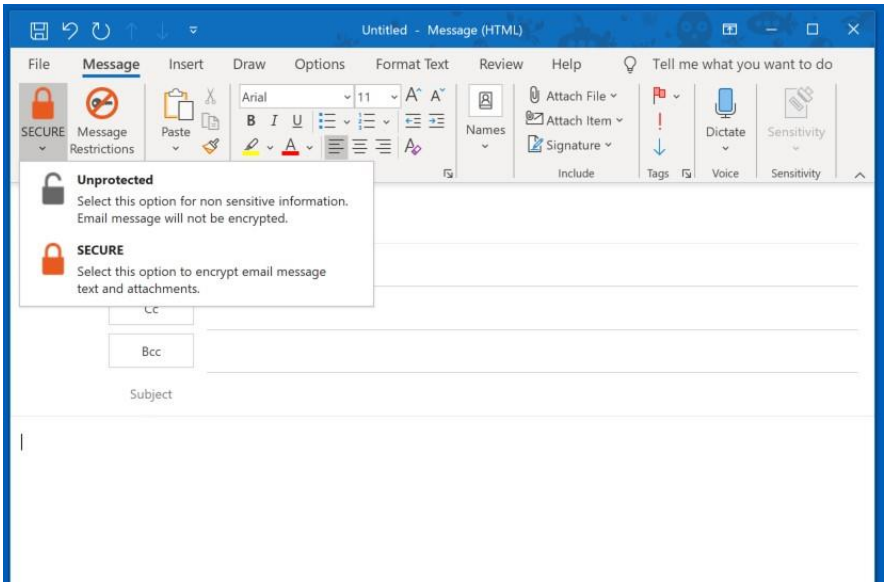
- **revoke access -** you instantly remove the recipient's ability to open the email or any attachments
- **control who can access the email and when** - modify this list of people and / or time restrictions in real-time meaning changes will take place immediately
- **view audit logs -** audit logs display all information about a secure email package including who has accessed it, when and where from. Failed attempts are also logged.

Egress Outlook add-in

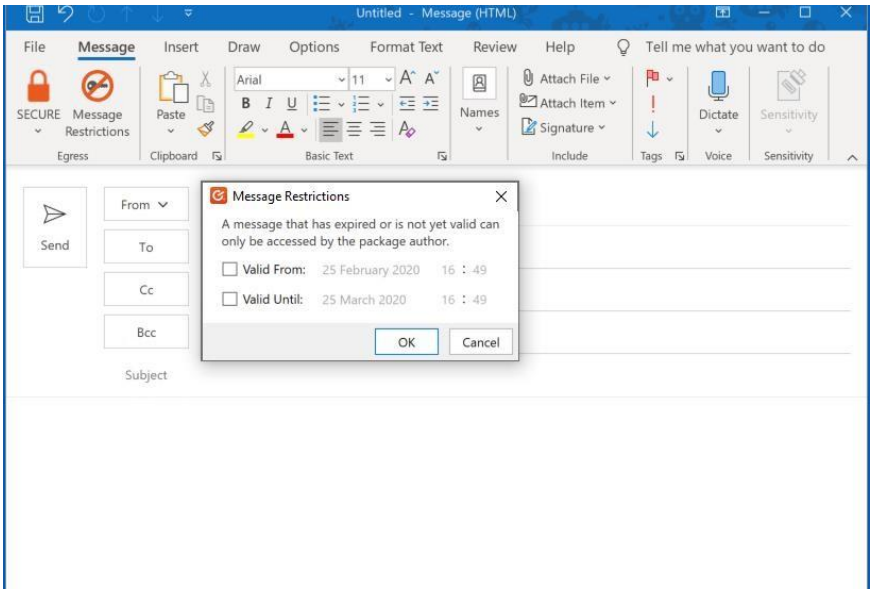
In addition to being able to send encrypted emails using [secure], NHSmail users who use Outlook to access their email accounts can download a free Outlook tool (known as an addin). This enables users to send encrypted emails without using [secure].

Information on how to download the Egress Outlook add-in is available on the NHSmail support site. Further information on deployment of the Egress Outlook add-in is available in the NHSmail Egress Outlook Add-in Desktop Deployment Guide.

Once downloaded and installed successfully, you can use the Egress Outlook add-in to encrypt emails by clicking on the open padlock icon in the top left of a new email and selecting the **SECURE** icon as per the screenshot below. Your email will then be encrypted once it is sent.



There is also an option to add date and time restrictions meaning that the recipient can only access the encrypted email and any attachments within the time that you select on the **Message Restrictions** icon as per the screenshot below. Please note this is optional and not required to send an email encrypted.



Egress large file transfer Outlook add-in

In addition to the features of the standard Egress Outlook add-in, a version of the Outlook add-in is also available that allows for large file transfers to non-NHSmail addresses or to other NHSmail users. The recipient does not need to have the Egress large file transfer Outlook add-in installed.

Information on how to download the Egress Outlook large file transfer add-in is available on the NHSmail support site.

The large file transfer feature works by uploading the file to Egress' secure cloud storage. The recipient receives an email that includes the link to access and download the file - this email will be the same size as an email without attachments, regardless of the size of the files being sent.

Note: If the recipient is an NHSmail user who does not have the add-in installed, the NHSmail recipient will need to follow the link in the email and login to the NHS Egress portal with their NHSmail credentials to access the large file. They will not be able to reply via the NHS Egress portal but can reply as normal using NHSmail.

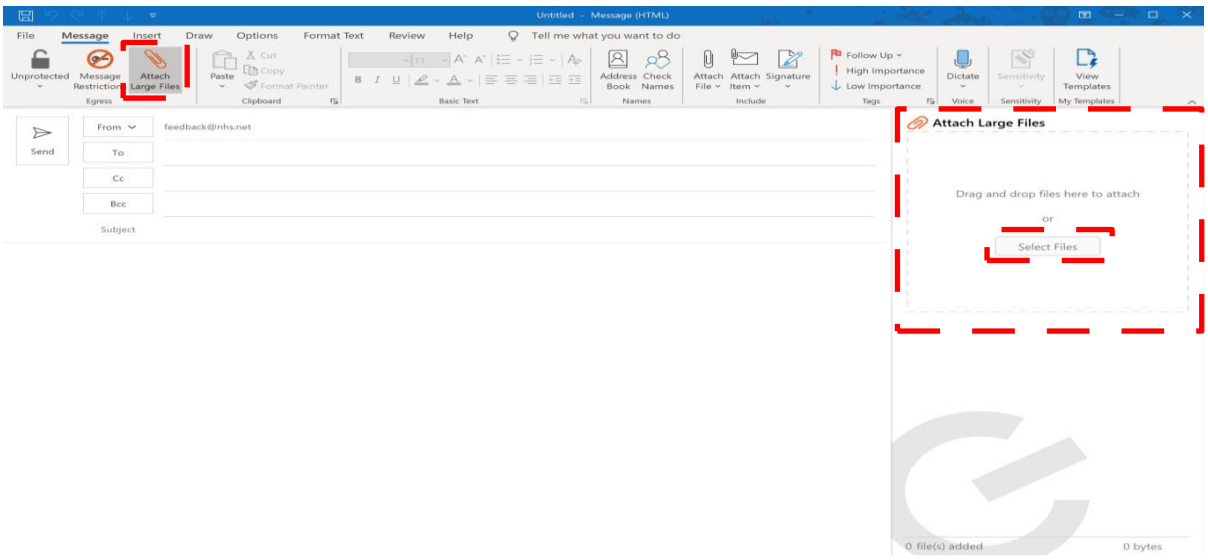
How to attach a file when sending by Egress large file transfer:

1. Select **Attach Large Files** within a new email as shown in the below screenshot.

   Files can be dragged and dropped into the **Attach Large Files** box that will show on the righthand side as below.

   Alternatively, files can be attached by browsing your computer using **Select Files.**

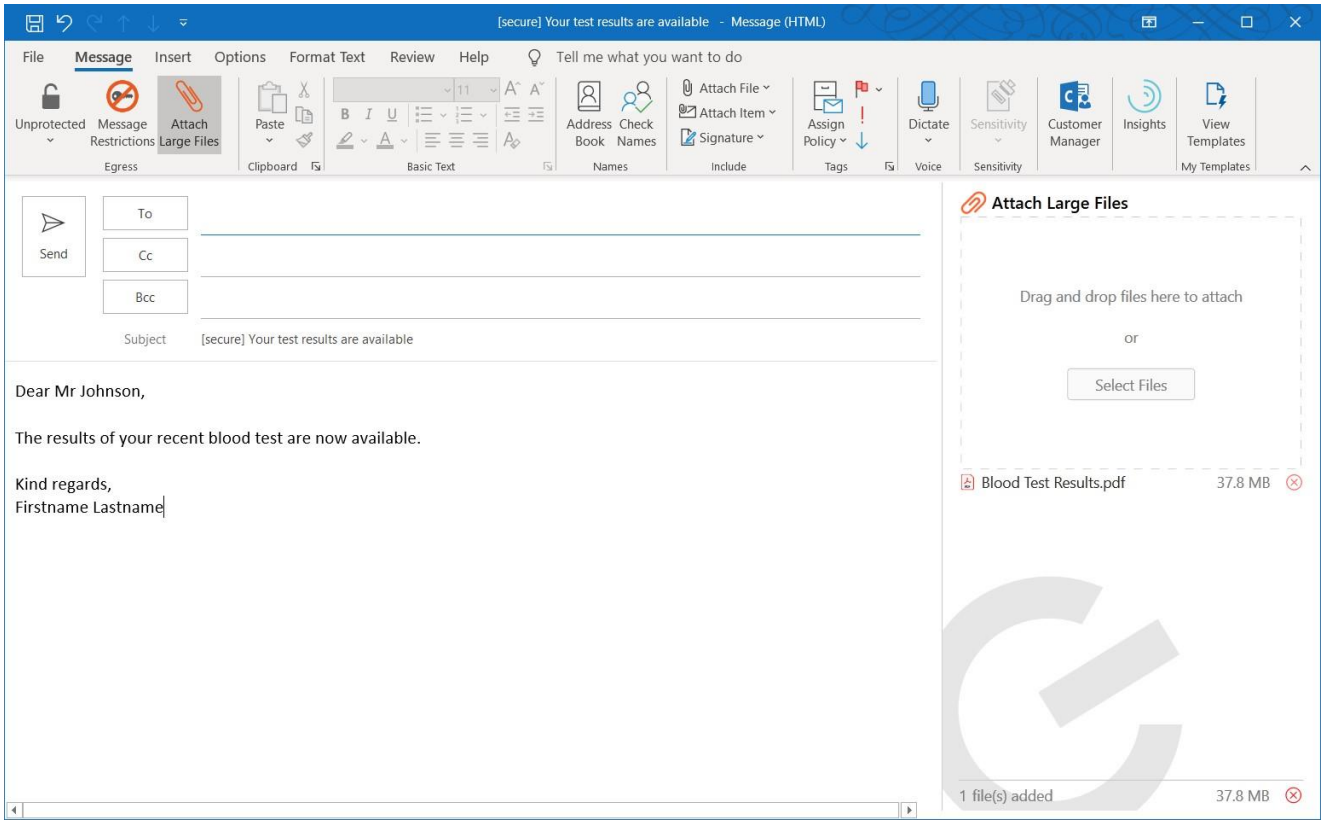
Example email using Egress large file transfer Outlook add-in



Note: Any files attached via the Egress **Attach Large Files** icon will be sent via large file transfer and the recipient will need to login to Egress to view these, even if the files are less than 35MB.

Note: Please refer to your local policies on sending large files to external organisations.

Example email using large file attachment



Egress large file transfer web form

NHSmail users can securely send large file transfers via the Egress large file transfer web form up to a maximum combined file size of 5GB without needing to download the add-in. This can be used to send to external recipients or other NHSmail users.

Please note: It is not possible to send a large file transfer from or to a shared mailbox as shared mailboxes do not have passwords and are not able to login to the web form to send an email or the Egress NHSmail portal to view the sent item.

For further information please see the Egress large file transfer web form guidance.

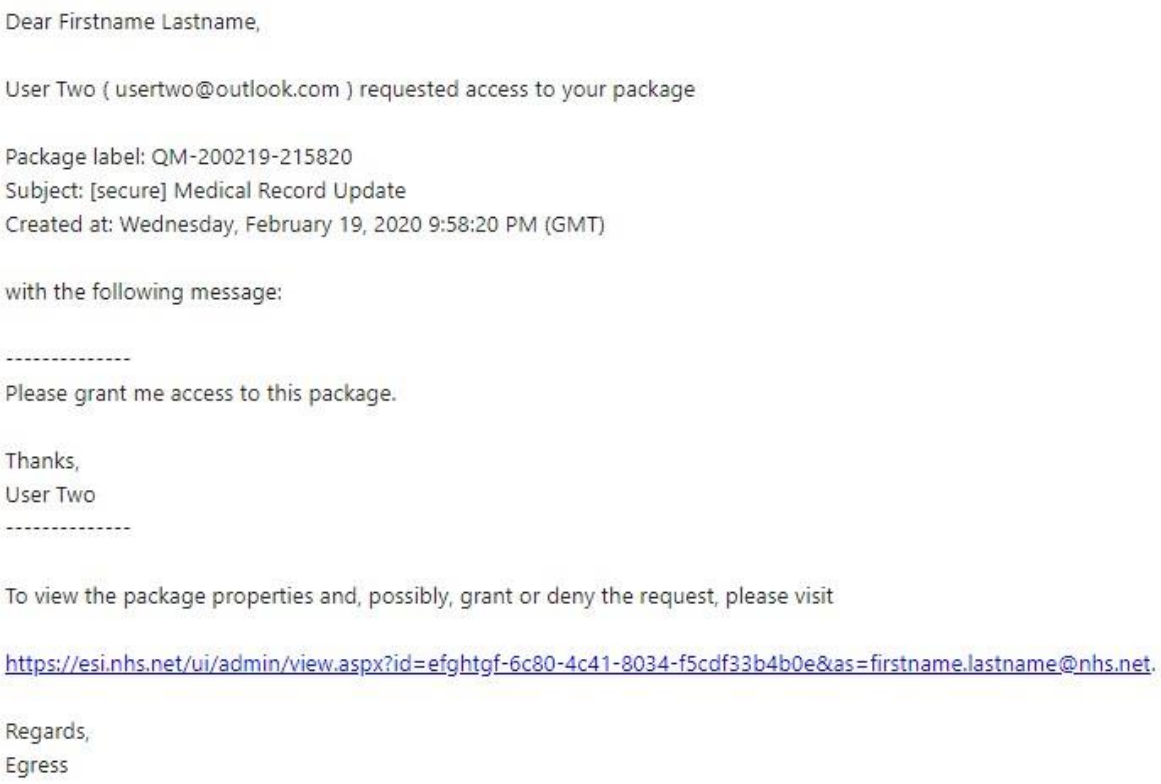
Approving access for others to secure emails sent via Egress

If the recipient forwards the encrypted email notification to another individual and they were not the original recipient(s), in order to get access to the encrypted email they will need to request access from you as the original sender.

They can do this by creating an Egress account - further information on how to do this is available in the accessing encrypted emails guide for non-NHSmail users.

You will receive an email notification to your NHSmail account that someone has requested access to a 'secure package' that you have sent. This refers to the encrypted email and any attachments that were sent encrypted. You are then able to approve or deny access to that individual, based on whether they have a genuine need to receive and view the content.

Example email requesting access to a secure email sent



Dear Firstname Lastname,

User Two (usertwo@outlook.com) requested access to your package

Package label: QM-200219-215820
Subject: [secure] Medical Record Update
Created at: Wednesday, February 19, 2020 9:58:20 PM (GMT)

with the following message:

Please grant me access to this package.

Thanks,
User Two

To view the package properties and, possibly, grant or deny the request, please visit

https://esi.nhs.net/ui/admin/view.aspx?id=efghtgf-6c80-4c41-8034-f5cdf33b4b0e&as=firstname.lastname@nhs.net.

Regards,
Egress

Note: Please refer to your local policies on sending sensitive information.

Help and further guidance

Help	Contact
Support for encrypted emails and Egress.	Egress support desk: 0844 800 0172 http://www.egress.com/support
Recipients of NHSmail encrypted emails who require help with registration.	Refer to: Accessing encrypted emails guide for non-NHSmail users Egress support desk: 0844 800 0172 http://www.egress.com/support
Other NHSmail queries	NHSmail helpdesk: 0333 200 1133 helpdesk@nhs.net

Frequently asked questions

Where is the data processed?
Data is encrypted on the NHSmail platform within the United Kingdom (UK).

When a recipient of encrypted email authenticates to the Egress encryption service to open the encrypted content or uses the Egress Outlook add-in (Egress software used to encrypt and access encrypted files), these actions are processed in the UK.

The encrypted email is stored within UK data centres for 90 days, to allow users to access it via the Egress Web Portal. Once encrypted, the reply is only unencrypted when it arrives on the NHSmail platform within the UK.

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.

Why do some of my pages on a document appear to be missing?
Large documents may not be able to be fully viewed from the Egress Web Portal, please download the document if you perceive pages are missing.

Is message tracking (for example, delivery or read receipts) available on encrypted emails?
Yes. Full audit events are available within the Egress Web Portal to see who has accessed the secure email and when.

Do I have to register for the service to decrypt replies?
No. As an NHSmail user, replies are received encrypted into the NHSmail data centre where they are decrypted and delivered to your inbox as normal.
If receiving a large file transfer you will need to login to the Egress Web Portal to view and download the files. You can do this by clicking the link in the email notification you will receive and then logging in with your NHSmail credentials.

Can I set up an application linked to NHSmail which will send automated encrypted emails?
Yes. The subject line must contain the encryption keyword [secure] and the application must be locally signed off for clinical use.

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

What is the maximum attachment size I can send by encrypted email replies or forwards?
This is 35MB however, if you install the Egress large file transfer Outlook add-in the maximum file size will increase to 5GB. You can also use the Egress large file transfer web form to send large file transfers, again with a maximum combined file size of 5GB.

What types of attachments can be included on encrypted email replies and 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.