Health & Social Care Information Centre

NHSmail
the secure communication solution

Sending an encrypted email from NHSmail to a non-secure email address

January 2015

V0.3

Copyright © 2013, Health and Social Care Information Centre.

Contents

Copyright © 2014, Health and Social Care Information Centre.

Introduction

NHSmail includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services.

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.

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.

NHSmail users can also exchange sensitive/patient information securely with users of the other secure Government domains[1] (referred to as the secure email boundary), provided the processes detailed in the NHSmail Acceptable Use Policy (AUP) are followed (http://systems.hscic.gov.uk/nhsmail/policies).

If users need to exchange information securely outside of the above secure email boundary, they can do so by using the NHSmail encryption feature. Encryption should primarily be used to exchange sensitive data as part of an agreed clinical workflow, and users should follow any local Information Governance policies that in place locally for sending sensitive data.

Note: sending an encrypted e-mail to secure government email address may result in non-delivery as email to these addresses is already secure.

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 safely verify the correct recipient.

1. First, send the recipient the 'Encryption Guidance for recipients' document which you can find in the NHSmail Training and Guidance pages at: https://web.nhs.net/Portal/InformationGuidanceServices/DefaultPage.aspx in the section 'Emailing sensitive or patient identifiable information'.

2. Next, follow the steps below to send an initial encrypted email but do not include patient or sensitive information. Once the recipient of the information has registered for the encryption service and confirmed to the sender this has been done, patient and sensitive data can be sent within an email or as an attachment subject to local information governance policies.

[1] For the full list of secure domains see the NHSmail training and guidance pages (https://web.nhs.net/Portal/InformationGuidanceServices/DefaultPage.aspx) in the section 'Emailing sensitive or patient identifiable information'.

Copyright © 2014, Health and Social Care Information Centre.

3. To send an encrypted email, log into your NHSmail account (either via an email client such as Outlook or via the web portal at www.nhs.net) and create a new email message in the normal way.

4. Ensure the recipient's email address is correct

5. In the **Subject** field of the email, enter the word [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.

6. Compose the message

7. Add any required attachments (once the initial registration process has taken place)

8. Click on **Send** to send the message. An unencrypted copy will be saved in your **Sent Items** folder.

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.

N.B. [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.

- There are a number of attachment types which aren't permitted to be sent via NHSmail, these include .exe files. If a non-permitted attachment is detected it will automatically be

Copyright © 2014, Health and Social Care Information Centre.

removed. For the full list of non-permitted attachments see the NHSmail training and guidance pages (https://web.nhs.net/Portal/InformationGuidanceServices/DefaultPage.aspx) in the section 'Policy and Procedure' / 'Blocked file extensions and attachments'.

Please note: it is your responsibility, 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. You should retain unencrypted copies of any encrypted email received in your local information repositories.

Help and further guidance

For help please visit the Trend Micro support site at:
http://www.privatepost.com/support/faqs.aspx

Or 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 help provided on the registration website.

Frequently asked questions

Q: Where is the data processed?

A: 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.

Q: Does the encryption feature work when NHSmail is accessed on all browser types and devices?

A: Yes.

Q: Is message tracking (e.g. delivery or read receipts) available on encrypted emails?

A: No.

Q: Do I have to register for the service to decrypt replies?

A: 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.

Q: Can I set up an application linked to NHSmail which will send automated encrypted emails?

Copyright © 2014, Health and Social Care Information Centre.

A: Yes, as long as the subject line contains the encryption keyword – [Secure] and the application is locally signed off for clinical use.

Q: Can encrypted replies received by generic mailboxes be accessed as normal?

A: Yes.

Q: What is the maximum attachment size I can send on encrypted email replies / forwards?

A: 20Mb

Q: What types of attachments can be included on encrypted email replies / forwards?

A: Certain file types are blocked by the NHSmail service and cannot be sent or received. The list of blocked attachments can be found on the NHSmail training and guidance pages (https://web.nhs.net/Portal/InformationGuidanceServices/DefaultPage.aspx) in the section 'Policy and procedure / Blocked and allowed attachments'.

Q: Is the service suitable for urgent, real time communication?

A: 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 using the service design mitigations through their business processes around loss of messages or being unable to open them.

Q: Can the service be used to communicate with nhs.uk email addresses?

A: 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.

Copyright © 2014, Health and Social Care Information Centre.