Sharing Sensitive Information Guide for NHSmail

January 2018
Version 4

Contents

Introduction

1.1. Purpose of Document

Target Audience: All end users of NHSmail

No unencrypted patient identifiable data should be transferred electronically across health and social care organisations. This document details how patient identifiable information should be securely exchanged via email and Instant Messenger and Presence.

Precautions have been taken to ensure that emails sent from NHSmail are secure. It is the sending email system's responsibility to ensure that appropriate safeguards have been applied for the sensitivity of the email being sent.

Sharing sensitive and patient identifiable information by email

1.2. NHSmail (*.nhs.net)

NHSmail is a secure national collaboration service which enables the safe and secure exchange of sensitive and patient identifiable information within NHSmail and from NHSmail to other suitably accredited email systems. The service also provides the facility to securely exchange information with insecure or non-accredited email services via the NHSmail encryption feature.

All user connections to the service are encrypted. The service operates out of secure, government-rated data centres to provide maximum levels of resilience.

Using NHSmail ensures the message is readable by authorised recipients, does not require any special software and removes the need to encrypt or password-protect attachments.

1.3. Across Health and Social Care

NHSmail provides an easy way to transmit patient data to other NHSmail users without the need to encrypt content.

Note: *secure.nhs.uk is the domain for local accredited NHS email services and sensitive data can be shared without further encryption. All other *nhs.uk email addresses are not secure and should not be used for exchanging unencrypted patient or sensitive data with.

1.4. Using NHSmail to email central and local government

Email sent to legacy secure government domains (see below) and any domain that is accredited to the government secure email standard or the SCCI 1596 secure email standard will automatically be sent securely and directly to the recipient's email system. NHSmail works with the Government Digital Service (GDS) and updates the list of accredited domains regularly.

The legacy secure domains are:

*.gcsx.gov.uk for local government
*.gsi.gov.uk and *.gsx.gov.uk for central government
*.cjsm.net and *.pnn.police.uk for Police/Criminal Justice
*.mod.uk for Ministry of Defence

Note the legacy local and central government email domains (gcsx.gov.uk, gsi.gov.uk and gsx.gov.uk) will slowly stop being used and then switched off completely in March 2019 as all local and central government organisations migrate to using .gov.uk email addresses for all email communication, after they have accredited these email addresses to the government secure email standard. Accredited .gov.uk email addresses will be whitelisted by GDS to demonstrate their compliance and this list of accredited email addresses will continue to be shared with NHSmail.

Any domain that is accredited to either standard, government secure email standard or the SCCI 1596, is suitable for sending OFFICAL-SENSITIVE information.

1.5. Emailing contacts using insecure or non-accredited email services

Note: please ensure you are familiar with the NHSmail Encryption guidance and process, before attempting to use the NHSmail encryption feature. Users should also comply with local governance processes and ensure they have permission to use the NHSmail encryption tool.

NHSmail encryption feature

The NHSmail encryption feature allows users to securely exchange sensitive information with users of non-accredited or non-secure email services. This means users can communicate securely across the entire health and social care community including emails ending in Hotmail, Gmail, Yahoo, .nhs.uk or any other type of email account.

Please note that *.secure.nhs.uk is accredited as being secure and can be used to receive sensitive information without the need for further encryption.

With the NHSmail encryption feature:

- NHSmail users can easily communicate securely with users of ANY email service without having to manually encrypt sensitive information
- Attachments are automatically encrypted and remain secure

- Users of non-accredited or non-secure email services can communicate securely with NHSmail users.

Using the NHSmail encryption feature if you are an NHSmail user

Note: before attempting to use the encryption service, please read the Encryption guide for NHSmail.

If you have a contact that uses a non-accredited or non-secure email service (e.g. ending .nhs.uk (excluding *.secure.nhs.uk), Hotmail, Gmail or Yahoo) and you need to exchange sensitive information with them, you will need to open the communications channel by sending an initial encrypted email, with [secure] in the subject line, that they can then open, read and reply to securely. If it is the first time they have received an encrypted email from an NHSmail account, they will have to register for the service before being able to read the email. Once the initial email has been sent and replied to, the channel has been created and sensitive information can be sent securely.

Using the NHSmail encryption feature if you are a user of an insecure email service

Note: before attempting to use the encryption service, please read the Accessing Encrypted Emails Guide.

To send an encrypted email to an NHSmail user, they must email you first. You can then reply to, or forward their email and it will remain encrypted. You can also include attachments.

Direct your NHSmail contact to the Accessing Encrypted Emails Guide on the NHSmail support pages, so that they can set up the communications channel with you.

When you have received an encrypted email from an NHSmail user, before you open, read and reply to it, you will need to register for an account with the NHSmail encryption provider. Step-by-step instructions can be found in the Accessing Encrypted Emails Guide for Non-NHSmail Users. Instructions will also be included in the email notification that you will receive.

Providers of publicly funded healthcare in England that have a requirement to regularly exchange sensitive and patient identifiable information outside of the NHS, government and social services may be eligible to apply for NHSmail accounts. The NHSmail Access Policy contains details and information on applying for accounts.

Your organisation may have existing processes and systems in place. You should only use the NHSmail encryption capability if approved to do so by your organisation and only in accordance with your local information governance policies and procedures.

1.6.Encrypted attachments and NHSmail

NHSmail users can also use encrypted attachments to send sensitive or patient identifiable information to users of insecure or non-accredited email services. Receiving organisations must ensure they have risk mitigation methods in place against malicious content or virus infected files that could be hidden in the encrypted file.

When an encrypted attachment is sent, the recipient will be alerted slightly differently depending on the email service that they are using:

From	To	Information
NHSmail (nhs.net)	NHSmail (nhs.net) or *.secure.nhs.uk	Encrypted attachments can be sent. No alert is generated. However, NHSmail to NHSmail is a secure route and there is no need for attachments to be encrypted.
nhs.net	Suitably accredited domains (see section two of this document)	Encrypted attachments should not be sent and may be silently removed. This means your data may not be received by the recipient.
nhs.net	nhs.uk	Encrypted attachments can be sent. Recipient is alerted. **Note: *secure.nhs.uk is the domain for local accredited NHS email services and sensitive data can be shared without further encryption**
nhs.net	Any email address other than those above	Encrypted attachments can be sent. Recipient is alerted.

Note: where the recipient is alerted, they will receive the attachment and the following warning message will be displayed in the body of the email:

> "The attachment named <NameOfFile>.zip could not be scanned for viruses because it is a password protected file"

While NHSmail allows you to send encrypted attachments, some receiving systems routinely block them as they are increasingly being used to send malicious content. When sending encrypted attachments, you should verify that the recipient is able to receive them.

1.7.Local secure NHS email services

The transmission of patient identifiable information **FROM NHSmail TO a secure local NHS email system** (*.secure.nhs.uk) is secure and does not require any further encryption.

1.8.Local insecure NHS email services

The transmission of patient identifiable information **FROM NHSmail TO an insecure local NHS email system** (*.nhs.uk) is only secure if the NHSmail encryption feature is used.

Transmission of patient identifiable information **FROM a local NHS email system (*.nhs.uk) TO NHSmail** should not be regarded as secure unless it is a reply to an NHSmail encrypted email originally sent to the local NHS email system by an NHSmail user.

Not only should the sender ensure that they use a suitably encrypted method to send the patient information, but that the receiving system is running a secure service so that the patient information remains confidential.

Automated forwarding of emails to any insecure domains, including local NHS email system (*.nhs.uk), from an NHSmail account is not permitted. NHS.uk and any other non-secure domain accounts are considered insecure and should never be used for the exchange of

sensitive data. Individual emails can be manually forwarded, if required, as long as there is no sensitive data contained within the email.

Emails from a local NHS email system (*.nhs.uk) can be forwarded onto an NHSmail account, if required. Please ask your local IT helpdesk / Local Administrator for guidance on how to do this.

1.9.Encryption standards for local solutions

A comprehensive, technical, good practice guideline of 'Approved Cryptographic Algorithms' (techniques for encoding data) has been produced by NHS Digital. This can be viewed by following the link below:

http://systems.digital.nhs.uk/infogov/security/infrasec/gpg/acs.pdf

When sending patient data, health and social care organisations should undertake a local risk assessment on each email system they send to in terms of its secure operation, availability and the method of data exchange. The outcome of the risk assessment must be reported to the organisation's Board, to ensure that the Board is aware of any risk before accepting responsibility/accountability for the decision to accept any data vulnerability/virus infection.

1.10. SCCI1596 secure email specification

The SCCI1596 Secure Email Specification defines the minimum requirements for secure email systems in health, public health and adult social care. A local email system that meets these requirements will be accredited to a level that will enable the secure transmission of patient identifiable data and sensitive information to the other secure email domains. Further information can be found in the Secure Email specification document.

Sharing sensitive and patient identifiable information by NHSmail Instant Messaging and Presence

Instant Messaging and Presence (IM&P) provides an instant messenger service as part of the NHSmail core service. The exchange of patient or sensitive information using the instant messenger tool is secure but should only be carried out in accordance with your organisation's local information governance policy and procedures.

An instant messaging conversation should be treated in the same way as a telephone conversation; after discussing any patient information via IM&P, users will be expected to properly document a record of all relevant conversations within the patient health record. Local organisations must ensure their staff meet professional standards for clinical documentation following use of IM&P.