Sharing Sensitive Information by Email –

A guide for Health and Social Care Email Users

February 2019
Version 1

Contents

Purpose of Document

Target Audience: All Health and Social Care Staff using NHSmail

This guidance has been designed to help avoid the use of fax machines or the postal service, to safely and efficiently share personal confidential data and sensitive information where there is a business need to do so by email or Instant Messenger.

A single page summary is included in Appendix 1.

Personal confidential data and sensitive data should be encrypted when sharing by email and assurance sought that the receiver will have appropriate safeguards in place to protect the data upon receipt.

This guide helps senders easily identify which email addresses are known to be secure (protected in transit and upon receipt) and which ones need additional protection when sending personal confidential data and sensitive information.

Summary Guidance

The table below is a summary of email addresses that are known / not known to be secure.

Email to secure addresses are encrypted in transit and the receiving organisation has committed to protect the data upon receipt.

Recipient email address ends	Secure	Additional actions required
*.nhs.net	Yes	Secure – no additional action required
*.secure.nhs.uk	Yes	
*.nhs.uk (does not end secure.nhs.uk)	Unknown	Use [secure] in the subject line
*.gov.uk	Yes	Secure – no additional action required
*. cjsm.net	Yes	
*.pnn.police.uk	Yes	
*.mod.uk	Yes	
*.parliament.uk	Yes	
Any other email address	Unknown	Use [secure] in the subject line

Detailed Guidance

About NHSmail

NHSmail is accredited to the DCB1596 Secure Email Specification and is a secure national collaboration service which enables the safe and secure exchange of personal confidential data or sensitive data within NHSmail and from NHSmail to other suitably accredited email systems. NHSmail 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 located in the UK, to provide maximum levels of resilience.

Sending sensitive information to other NHSmail users

Apart from ensuring you have the correct recipient, no additional action or protection is required.

Organisations that use NHSmail have committed to appropriately protect data on receipt as part of their Information Governance obligations.

Note: NHSmail email addresses end with “*.nhs.net”.

Sending sensitive information across Health and Social Care

Systems that meet the secure email standard
Locally run email services that meet the secure email standard need no additional action or protection apart from ensuring you have the correct recipient.

Organisations that have met the standard have committed to appropriately protect data on receipt as part of their Information Governance obligations.

Note: These systems have email addresses that end with “*.secure.nhs.uk”.

Systems that do not meet the secure email standard
All other “*.nhs.uk” email addresses have not yet met the secure email standard and should not be used for exchanging unencrypted personal confidential data or sensitive data.

Individuals needing to send sensitive information from NHSmail to a “*.nhs.uk” address that does not end with “*.secure.nhs.uk” should use the NHSmail encryption feature.

Note: These systems have email addresses that end with “*.nhs.uk” and do not include .secure.nhs.uk at the end.

Sending sensitive email across Government

Email sent to government email addresses will automatically be sent encrypted to the recipient's email system, providing their system accepts encrypted connections (note all government email services are required to support this).

Any government run email service has a statutory requirement to comply with the Government Security Policy Framework and the Data Protection Act 2018 / General Data Protection Regulation. Where government organisations comply with their statutory requirements, you are assured that the email will be appropriately protected on receipt and not need any additional protection.

Government organisations use a protective marking scheme and NHSmail is suitable for exchanging OFFICIAL and OFFICIAL-SENSITIVE protectively marked information.

The government addresses end with:

*.gov.uk" for local and central government
.cjsm.net" and ".pnn.police.uk" for Police/Criminal Justice
*.mod.uk" for Ministry of Defence
*.parliament.uk" for Parliament

Note local and central government historically used legacy email addresses ending with "*.gcsx.gov.uk", "*.gsi.gov.uk" and "*.gsx.gov.uk" which are scheduled for switch off in March 2019. Local and central government organisations will instead switch to using "*.gov.uk" email addresses.

Sending sensitive information to any other system

Note: Any other email address not listed above is not known to be secure.

The NHSmail encryption feature allows NHSmail users to securely exchange personal confidential data with users of non-accredited or non-secure email services. This means users can communicate securely to any type of email account and across the entire health and social care community as well as to patients / citizens.

It is invoked by putting [secure] in the subject line of a message with the inclusion of the square brackets.

Before using the service:

- check local organisation policies and processes on sharing personal confidential data and sensitive information first which will take precedence over this guidance
- ensure you are familiar with the NHSmail Encryption guidance and process

You should only use the NHSmail encryption capability if approved to do so locally.

Receiving sensitive information

Email services that meet the secure email standard and government email services should have been informed by their organisation that it is safe to send personal confidential data to NHSmail without any additional protection.

In line with the NHSmail Acceptable Use Policy and your organisation's Information Governance policies / procedures you will have received guidance and training in how to manage sensitive information and ensure it is protected after receipt.

Electronic and digital signatures

In many instances people need to supply a simple text signature on an email to confirm it has come from them in their official capacity, in the same way they would on a letter or fax. In nearly all cases, ending the email in the same way as you would with a letter is enough:

Name
Job title / role
Organisation

To help avoid forged or spoofed emails where the email has been sent from another email system pretending to be from NHSmail, the service applies technical protections to help avoid this. These include NHSmail informing other email systems of the unique network addresses NHSmail sends its email from and asking them to ignore email if it has come from somewhere else, as well as digitally signing every email sent to let receiving systems know if the content has been tampered with.

Instant Messaging

NHSmail includes an instant messaging service at no additional cost. The exchange of personal confidential data using the instant messenger service is secure but should only be carried out in accordance with your organisation's local Information Governance policies and procedures.

As detailed in the NHSmail clinical safety case, an instant messaging conversation should be treated in the same way as a telephone conversation; after discussing any patient information via this service, 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 the service.

Appendix 1

NHSMAIL SENDING SENSITIVE INFORMATION QUICK GUIDE

These domains are secure (no further action)

- nhs.net
- secure.nhs.uk
- gov.uk (no longer needs to be gsi.gov.uk)
- cjsm.net
- pnn.police.uk
- mod.uk
- parliament.uk

Put [secure] in the subject line if sending personal confidential data or sensitive information to

- nhs.uk (if it doesn't end in secure.nhs.uk)
- any other email address

Always check your local organisation policies and processes on sharing personal confidential data and sensitive information first which will take precedence over this guidance.

See more detailed guidance at https://portal.nhs.net/Help/policyandguidance