Sharing Sensitive Information by Email –

A guide for Health and Social Care Organisations

November 2019

Version 2

Contents

Purpose of Document

Target Audience: All Health and Social Care Organisations

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 and instant messenger.

Personal confidential data and sensitive information 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 provides organisations with information to help them comply with their Information Governance obligations.

DCB 1596 secure email specification

The DCB1596 Secure Email Specification defines the minimum requirements for secure email systems in health, public health and social care. A local email system that meets these requirements will be accredited to a level that will enable the secure transmission of personal confidential data and sensitive information to the other secure email domains. Further information can be found in the secure email specification document.

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

Signatures should only be accepted from systems that have met the secure email specification as these have employed measures to help avoid forged or spoofed emails where the email has been sent from another email system pretending to be from the authorised email service.

These technical measures include informing other email systems of the unique network addresses their system sends its email from and asking them to ignore email if it has come from somewhere else (Sender Policy Framework (SPF) as well as digitally signing every email sent to let receiving systems know if the content has been tampered with (Domain Keys Identified Mail (DKIM).

For organisations that use NHSmail

NHSmail is accredited to the DCB1596 Secure Email Specification. It is a secure national collaboration service which enables the safe and secure exchange of sensitive and personal confidential data within NHSmail and from NHSmail to other suitably accredited email systems

with encryption to those systems that support it. 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 NHSmail service are encrypted. The service operates out of secure, government-rated data centres located in the UK, to provide maximum levels of resilience.

NHSmail sends all email encrypted to receiving systems that support encryption. Providers of publicly funded healthcare in England that have a requirement to regularly exchange personal confidential data and sensitive 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.

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

Recipient email address ends	Secure	Additional actions required
*.nhs.net	Yes	Secure – no additional action required
*. nhs.uk domains accredited to the DCB1596 secure email standard).	Yes	
*.nhs.uk (not accredited to the DCB1596 secure email standard)	Unknown	Use [secure] in the beginning or end of the subject line
*.gov.uk	Yes	Secure – no additional action required
*. cjsm.net	Yes	
*.police.uk	Yes	
*.mod.uk	Yes	
*.parliament.uk	Yes	
Any other email addresses (which have not accredited to the DCB1596 secure email standard)	Unknown	Use [secure] in the beginning or end of the subject line

Sending sensitive information to other NHSmail users

Apart from users ensuring they 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 email 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 the user is sending to 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 and email addresses are listed on the DCB1596 secure email standard website.

Systems that do not meet the secure email standard

All other "*.nhs.uk" email addresses that have not yet met the secure email standard and are not listed as accredited should not be used for exchanging unencrypted personal confidential data and sensitive information.

Individuals needing to send personal confidential data and sensitive information from NHSmail to a "*.nhs.uk" address (not on the accredited list), should use the NHSmail encryption tool.

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 "*.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 was 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 and sensitive information 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 placing [secure] at the beginning or end of the message's subject line, including 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 and sensitive information 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 personal confidential data and sensitive information and ensure it is protected after receipt.

Instant Messaging

NHSmail includes an instant messaging service at no additional cost. The exchange of personal confidential data and sensitive information 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.

Summary information for NHSmail users

A guide for NHSmail users has been provided separately and includes a one-page summary that users can keep for useful reference.

For organisations that run their own email service

In the first instance, all organisations should prioritise removing unaccredited email solutions and either achieving conformance to the DCB1596 Secure Email Specification or use one of the services that have already met the standard.

Having an accredited service will mean other organisations will be able to easily exchange personal confidential data and sensitive information with your organisation.

While organisations work to complete this conformance, they can still use email for sharing personal confidential data and sensitive information provided the organisation takes additional steps to protect the information being shared and have conducted a local clinical and information risk assessment.

Best practice guidance is provided by the Information Commissioner's Office (ICO) and can be found at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-tothegeneraldataprotection-regulation-gdpr/encryption/encryption-scenarios/

Best practice guidance for clinical safety can be found at:

https://digital.nhs.uk/services/solution-assurance/the-clinical-safetyteam/clinicalriskmanagement-standards

Sending personal data by email

By necessity the TO, FROM, DATE and SUBJECT fields of an email are transmitted in plaintext and may be accessed by any unintended recipient or third-party who intercepts the communication. Without additional encryption methods in place, the email body and any attachments will also be accessible to any unintended recipient or third-party who intercepts the communication.

A common type of personal data disclosure occurs when an email is sent to an incorrect recipient. You should be aware that encryption will only provide protection to personal data sent by email if the incorrect recipient does not have the means to decrypt the data (e.g. does not have the decryption key).

Personal data can also be at risk if an individual gains unauthorised access to the email server or online account storing emails which have been read or are waiting to be read.

The choice of password-securing the server or email account is similarly important when considering the security requirements of the email system.

Encrypted email

Encrypted email can provide the capability to encrypt the body and attachments of emails. For example, OpenPGP and S/MIME standards are widely used encryption methods which have been implemented by a range of free and commercial software products.
The sending and receiving of encrypted email requires the use of compatible email client software and requires configuration in advance. A wide range of free and proprietary products are available for desktop, laptop and mobile operating systems. There are some specialist webmail providers which support encrypted email, but it is not generally supported by the majority of online email providers, although there are some browser plug-ins which can provide this capability and further progress is being made in this area.

Encrypted email uses asymmetric encryption and requires a user to generate a key pair before they will be able to send an encrypted email. Users will also have to exchange public keys before an encrypted email can be sent between them. The private key must be kept secret.

Encrypted attachments

Email can also send information by encrypted attachments. The file is encrypted using software on the sender's device and added as an attachment to a standard email.

This is similar in concept to sending data via USB devices or optical disks. In order to decrypt the attachment, the recipient must have compatible software (in some cases the same software) and have access to the key. Commonly the key is derived from a shorter, morememorable password which can be transferred to the recipient however, the password must be sufficiently long and complex to prevent compromise.

To achieve the maximum guarantees that can be offered by the use of encrypted attachments, the key must be communicated over a separate communication channel, e.g. by disclosing the password over the telephone upon confirmation that the email has been delivered. Including the password within the same email as the encrypted attachment affords little protection to the encrypted personal data.

Additional tools

In addition to the ICO guidance highlighted above, the National Cyber Security Centre (NCSC) have developed an open-source tool to test and report on email security for UK public sector domains.

MailCheck processes aggregate Domain-based Message Authentication, Reporting and Conformance (DMARC) reports and tests the configuration of anti-spoofing controls and support for Transport Layer Security (TLS) to encrypt email over Simple Mail Transfer Protocol (SMTP).

Appendix 1

NHSMAIL SENDING SENSITIVE INFORMATION QUICK GUIDE

These domains are secure (no further action)

- nhs.net
- All domains accredited to the DCB1596 Secure Email Standard
- gov.uk
- cjsm.net
- police.uk
- mod.uk
- parliament.uk

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

- nhs.uk (if not accredited to the DCB1596 Secure Email Standard)
- 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.