Sharing Sensitive Information by Email with Health and Social Care Organisations –

A guide for Government Organisations

February 2019
Version 1

Copyright © 2019 NHS Digital

Contents

Copyright © 2019 NHS Digital

Purpose of Document

Target Audience: Government organisations that need to exchange personal confidential data and sensitive information with 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 or instant messenger.

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

This guide provides government organisations with information on health and social care email services in England to help them comply with their Information Governance obligations.

DCB 1596 secure email specification

Within health and social care all organisations are legally obliged to give due regard to the DCB1596 Secure Email Specification. This standard 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. Accredited email system organisations are obliged to ensure their staff and systems appropriately protect the content of email upon receipt. The standard is based on ISO 27001:

- Suppliers of commercial services are required to achieve ISO 27001 certification
- Health and social care organisations running their own email service are required to self-certify ISO 27001 compliance using the Data Security and Protection Toolkit (this replaced the Information Governance Toolkit in 2018).

All services that meet the secure email standard are required to run regular IT health checks (penetration testing) and employ anti-spoofing measures including:

- Domain-based Message Authentication, Reporting and Conformance (DMARC).
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)

The standard is aligned to government email standards with additional requirements to support clinical safety within the email service.

There are two categories of service that meet the standard:

- NHSmail (*.nhs.net)
- Independently procured email services (*secure.nhs.uk)

Copyright © 2019 NHS Digital

These are detailed further in the following sections of this document.

The NHSmail service (*nhs.net).

NHSmail is a nationally provided and managed secure email service used by over 1.3 million health and social care staff.

All user connections to the NHSmail service are encrypted in line with National Cyber Security Centre (NCSC) encryption requirements. All administrators are required to use multi-factor authentication.

The best practices below are in place to protect data at rest and minimise the risk of data aggregation, in instances where a user connects to the service with a mobile device.

- Encryption is enforced on the device
- A password is enforced on the device and the device is locked after a period of inactivity
- The device is wiped after eight incorrect login attempts
- No attachments over 10 MB can be downloaded onto the device
- A maximum of 30 days of email can be stored on the device
- Administrators and users can remotely wipe a device if lost / stolen

The service operates out of multiple secure, government-rated data centres located in the UK, to provide maximum levels of confidentiality, integrity and availability.

NHSmail sends and receives all email encrypted between systems that support encryption using opportunistic Transport Layer Security (TLS) and is approved for OFFICIAL and OFFICIAL-SENSITIVE information. The service does not support enforced TLS connections for reasons of clinical safety. Failure of TLS on the link could prevent time-critical clinical information being delivered.

As a highly managed service, encryption runs at all times - should it not, there is a very low risk of email interception to a government email service. The service sends email with NCSC approved encryption ciphers / certificates. The service accepts connections from depreciated ciphers due to commodity software limitations. If your system only sends using NCSC approved encryption ciphers / certificates, then you are assured of an appropriate level of encryption.

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

A national clinical safety case is in place for the use of email with local workflows assured under local safety cases.

Copyright © 2019 NHS Digital

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

Locally procured accredited email services (*secure.nhs.uk)

Locally procured accredited email services are built and run locally by organisations or public cloud services purchased by organisations that have met the secure email standard.

All user connections to these systems are required to be encrypted. Services will be located where the organisation procuring the service has agreed - this could be outside of the UK in line with the organisation’s risk appetite, signed off by their Board.

Services are required to send and receive all email encrypted between systems that support encryption and are approved for OFFICIAL and OFFICIAL-SENSITIVE. Locally run systems will each have their own approach to opportunistic and enforced TLS connections subject to local policies / clinical safety requirements.

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

A local clinical safety case is in place for the use of email with each locally operated service.

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

Further information can be found in the Secure Email specification document.

Copyright © 2019 NHS Digital

Locally procured non-accredited email services (<organisation>secure.nhs.uk)

All other "*.nhs.uk" email addresses have not yet met the secure email standard. This means that the organisation has not yet asserted if it has:

- Transport Layer Security (TLS) in place to encrypt data in transit
- a suitably scoped Information Security Management System in place with a recent IT health check (penetration test) on its email service and network perimeter
- anti-forging / spoofing measures in place
- organisation compliance with Information Governance requirements to protect data upon receipt
- clinical safety procedures in place when using email

Should your organisation wish to exchange personal confidential data or sensitive information with an organisation that has not met the secure email standard, subject to your local risk appetite, you should:

- wait for the organisation to meet the secure email standard
- use local encryption tools and establish a joint data sharing agreement to address Information Governance and clinical safety

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

Note: In Scotland, locally run email services end *.scot.nhs.uk and in Wales *.wales.nhs.uk and operate their own email assurance programme.

Copyright © 2019 NHS Digital

Summary Guidance

Guidance issued to government organisations

Recipient email address ends	Secure
*.nhs.net	Yes
*secure.nhs.uk	Yes
*.nhs.uk (does not end secure.nhs.uk)	Unknown

Guidance issued to health and social care organisations

Recipient email address ends	Secure
*.nhs.net	Yes
*secure.nhs.uk	Yes
*.nhs.uk (does not end secure.nhs.uk)	Unknown
*.gov.uk	Yes
*. cjsm.net	Yes
*.pnn.police.uk	Yes
*.mod.uk	Yes
*.parliament.uk	Yes
Any other email address	Unknown

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).

Copyright © 2019 NHS Digital