

Using Email in NHSScotland: A Good Practice Guide

The aim of this document, the first specifically for NHSScotland, is to show what types of information can be shared via email with NHS colleagues, business partners and patients given the current technical constraints and level of risk. Associated safeguards are also described.

It supersedes any existing documentation either from Scottish Government, NHS National Services Scotland or any local interpretations of policies that derived from NHS England (e.g. former Connecting for Health Programme).¹ The guidance is based on NHSScotland's own assessment of actual risk and discussions with the Information Commissioner's Office on how to improve security while allowing necessary business to be conducted.² This risk-based approach, which places far more emphasis on improving handling instructions than just technical security, will inform board-level email and information-sharing policies.

Outcome aligned to eHealth Strategy: boards will be able share the appropriate amount of information, including sensitive personal data, with those who have a legitimate or legal right to view it and that proportionate measures, including technical security, are in place that are commensurate with the sensitivity of the information and the risk of loss or misuse.

¹ This supersedes for example any previous guidance relating to N3, NHSmail etc and focuses on areas where NHSScotland boards can agree on level of risk regardless of which email service is used. It is based on a consultation between August 2011 and April 2012.

² For example ICO Civil Monetary Penalties tend to relate to failures in user handling and process rather than because an email service did not use transport encryption.

What information can I send via email and to whom?

The aim of this guidance is to show what types of information can be shared via email with NHS colleagues, business partners and patients given the current technical constraints and level of risk. Three steps need to be followed

STEP 1: What is the sensitivity level of the information I wish to send or receive?

STEP 2: Have I checked the handling instructions (e.g. whether it is permissible to send and special instructions for emailing different parties including patients)?

STEP 3: Have I checked the email address of the recipient (e.g. nhs.net, nhs.uk, GSi etc.?) against the tables to see if the level of technical security allows this?

STEP 1: What is the sensitivity of the information?

All NHS information should be handled with care, especially that which contains personal data. But some types of information are more sensitive than others.

Deciding on whether email should be used, and what steps need to be in place before sending, depends on the relative sensitivity of the information and the impact that would be caused if the information were lost or sent to the wrong person for example.

Higher sensitivity is not determined simply by the type of document (e.g. X assessment form or Y appointment letter). Instead, a judgement needs to be made as to the impact that would be caused if the information was lost or misused.

Three levels can be used to describe the information which the NHS holds. For simplicity these can be viewed like traffic lights: **‘Green’**, **‘Amber’** and **‘Red’**.

GREEN: Unclassified information

This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person's name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person's physical or mental state.

AMBER: Protected information

In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:

- Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost.
- Any information which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result).
- Any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).

RED: Highly sensitive information

Most boards also hold some information which is highly sensitive. Particularly:

- Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way).
- Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health.
- Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file).
- Information relating to vulnerable persons' health (e.g. child protection cases)
- Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment).
- Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

Step Two: What are the handling instructions for email?

Greater care with circulation lists and group addresses

The vast majority of email-related privacy breaches have been the result of sending information to the wrong person. No amount of transport encryption would help here. This can be simply the result of choosing the incorrect name from an address list. Such human errors can never be removed entirely but can be reduced by switching off the auto-population of address functionality and far better controls on the creation and use of email address circulation lists (do you really need so many long 'cc' lists? Are they kept up to date? Are 'group addresses' clearly differentiated from individual persons' addresses when a user scrolls down the global email address book?).

Avoiding bulk transfers of personal data via email

Where there is a business need to send high volumes of patient identifiable information in one batch it is essential to consult Information Governance and Security leads beforehand as other means of transit are likely to be more suitable (e.g. encrypted media sent by tracked courier). If the bulk data is to be used for secondary/research purposes then there are also Caldicott procedures to follow (that includes sufficient data anonymisation).

GREEN: unclassified information

Such information can be sent to any email address, including via the Internet, to a person or organisation that has a legitimate business need to see.

AMBER: Protected information

- Email should only be exchanged between NHS colleagues and trusted partners with a legitimate or legal right to access the information.

Note: 'Unconnected organisations' are parties that NHSScotland boards have little or no contact with and have no pre-agreed information sharing protocols (i.e. could not be considered a trusted partner).

- Email should only be sent from official NHSScotland email accounts (i.e. NHS.net or NHS.uk) and not personal non-work related accounts.
- Email to patients can be made possible only if special conditions are met (see below).
- Information in a single email should only relate to one individual as far as possible. Take great care with 'group/circulation addresses' as most privacy breaches are the result of sending to the wrong persons.

RED: Highly sensitive information

- Email can only be exchanged between NHS colleagues and trusted partners with a legitimate or legal right to access the information **and** who are deemed to have adequate network security measures in place (see tables B and C below).
- Email should only be sent from official NHSScotland email accounts (i.e. NHS.net or NHS.uk) and not personal non-work related accounts.
- Email should **not** be used as a medium for communications with un-connected organisations, patients or the wider public.
- Information in a single email must only relate to one individual. Take great care with 'group/circulation addresses' as most privacy breaches are the result of sending to the wrong persons.

Emailing patients and the wider public

Email is one of several important communications channels with patients and the wider public. But as with paper letters there are security and practical issues to contend with (given that the NHS does not yet have services in place that can deal with high volumes of email securely). In the meantime, steps can be taken to make email possible as a form of communication if there is:

- **Patient consent³:** there must be prior consent that he/she would be prepared to accept certain types of communication via email. Often the demand comes from patients and the benefit of receiving an un-encrypted email (e.g. to confirm in writing that a consultant is available at short notice) outweighs the risk and impact of loss. In cases where there is incapacity a guardian with powers of attorney can make the decision. Patients must also understand that security of emails from the NHS cannot be guaranteed once they enter the Internet, hence for example their email service provider may hold copies on their servers and have their own security and access policies.
- **Agree purpose:** keep to pre-agreed communications at the lower end of the sensitivity scale such as:
 - 'Keeping in touch'
 - Appointments, queries and options for treatment
 - Where the patient has agreed that a relative abroad should be kept informed about progress
 - Reply to complaints and Freedom of Information requests
- **Manage expectations:** that email is only just one channel and that highly sensitive information (RED) would never be shared via email (i.e. telephone, face-to-face etc would still be required). If the email conversation begins to stray into more sensitive territory then other channels may be required.
- **Agree email address:** individuals often have multiple email accounts. Patient/public needs to keep the service informed of the correct email address. The chosen account should be tested before sending.

³ Patient consent is described in more detail in the NHSScotland *Code of Practice on Protecting Patient Confidentiality*. Consent can be implicit and explicit, written and un-written.

- **One email = one patient:** Keep the communication focussed on the individual who gave consent (i.e. not other third parties).
- **Never email medical records:** no case notes or clinical parts of the formal patient record should be emailed (either in the body of the text or as attachments).
- **Keep professional:** write as though this were any other form of clinical correspondence and do not mix personal life with business.
- **Records management:** work in accordance with board level record policies; consider whether the email needs to be filed in the formal record or deleted after a short period. Note: your 'sent' items are discoverable for the purposes of Data Protection subject access requests.

STEP 3: What information can be emailed to colleagues and partners outside the board?

Using the email address suffix

The tables below show whether email can be sent to different parties given the current level of known risk and technical security. Email exchanges between all official accounts (nhs.uk or nhs.net) *within NHSScotland* are considered as 'trusted'.⁴ For external partners (e.g. police, local government etc.) the tables shows whether email is permissible.

Many business partners, especially the emergency services, local and central government use the Government Protective Marking scheme.

Amber information is equivalent to PROTECT

Red information is equivalent to RESTRICTED

These two terms should be added to the title line of the email when emailing such external partners in accordance with an Information sharing protocol (but not mandatory when emailing NHS colleagues).

Note: partners using the Government Protective Marking Scheme will only be familiar with PROTECT and RESTRICTED so do not use other terms (e.g. NHS Confidential, 'in confidence' or 'personal') as this can lead to confusion.

⁴ Boards with NHS.UK email services for example typically have a relay to N3. N3 itself is not encrypted. Risks are mitigated through better handling instructions etc. rather than simply making a decision based on whether transport-encryption is in place.

Table A

Can I use email for protected (AMBER) information?

From any NHSScotland official email account to	Protected information AMBER Can I send or receive email?
Another official NHSScotland email address (nhs.net or nhs.uk)	✓
Trusted partner with GSi equivalency*	✓
Trusted partner without GSi equivalency*	✓
Patients and wider public (subject to ground rules, see above)	✓
Unconnected organisations	✗

* The term PROTECT may need to be added to the title line when you are emailing these external partners and Information Sharing protocols will specify ground-rules.

Can I use email for highly sensitive (RED) information?

Note: given the technical differences between NHSMail (which has suffix nhs.net) and NHS.uk services there is a separate table as the technical security is different.

Table B

NHSMail user: Can I use email for highly sensitive (RED) information?






From a NHSMail account to or from:	Highly sensitive information RED Can I send or receive email?
Another official NHSScotland email address (nhs.net or nhs.uk)	✓
Trusted partner with GSi equivalency+	✓
Trusted partner without GSi equivalency*	✗
Patients and wider public	✗
Unconnected organisations	✗

+you may be asked to use the term RESTRICTED when sending this level of information to your partner with a GSi email address as per local protocol.

* Consult IT Security; this highly sensitive Information (equivalent to RESTRICTED) needs to be sent as paper or encrypted memory stick via tracked postal services. Or other encryption methods.

Table C

NHS.uk user: can I use email for highly sensitive (RED) information?

From an NHS.uk account or to:	Highly sensitive information RED Can I send or receive email?
Another official NHSScotland email address (nhs.net or nhs.uk)	
Trusted partner with GSi equivalent*	
Trusted partner without GSi equivalency*	
Patients and wider public	
Unconnected organisations	

* Consult IT Security if you need to share data here; highly sensitive Information (equivalent to RESTRICTED) needs to be sent as paper or encrypted memory stick via tracked postal services. Or other encryption methods. No information marked CONFIDENTIAL (GPMS) should ever be emailed in NHSScotland.

Note on terms used:

- GSi stands for Government Secure Intranet; it is a wide area network used by many government bodies. It works on the basis of security accreditation and codes of connection. 'GSi-equivalency' shows where similar public networks are deemed to meet the same level of security.

Email suffix that is GSi equivalent	Example organisation
x.gsi.gov.uk gsi.gov.uk	Scottish Government; some staff in local authorities
gsx.gov.uk	Probation
pnn.police.uk ;	Police constabulary
cjsm.net	Courts
scn.gov.uk	Police
gcsx.gov.uk	Local authorities
mod.uk	Military base
gse.gov.uk	Government office

DMB