BrisDoc Patient care by people who care

NHS

Email Use and Third-Party Sharing Policy

Version:	Owner:	Created:
5.6	Deb Lowndes (Programme and Service Director)	1st March 2010
Published:	**Approving Director:**	**Next Review**
21/10/2025	Rhys Hancock (Director of Nursing, AHPs and Governance)	07/07/27

Contents

Contents

Document Purpose

This document sets guidance for email use and sharing of data with third parties. Each is dealt with separately but overall responsibilities and legal requirements apply to all information relating to the sending of patient/person identifiable, corporate and sensitive data. Information Governance Leads for each service / department are identified in the Information Governance Framework document and should be contacted if you are in doubt.

1. Overview of User responsibilities

You can -

- Send identifiable patient data or sensitive data relating to staff to other NHS organisations, in limited and controlled circumstances using NHSMail. If an NHSMail-to-NHSMail transfer cannot be achieved, this should be referred to the Information Governance Lead/Service Manager for approval and guidance.
- Data Processing Agreements (DPAs) must be in place with third parties and align with UK GDPR Article 28 requirements where data is being share that is sensitive or in bulk.
- NHSMail can send secure email to accredited domains (e.g., *.gov.uk, .police.uk)* under NHS Digital's Secure Email Standard.
    - https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email

You must not -

- Send identifiable patient data or sensitive data on staff outside the NHS without contacting the Information Governance Lead, SIRO or Caldicott Guardian and establishing a secure method of inter-agency communication.
- Make excessive personal use, make any personal gain, or undertake political or commercial activities.
- Send or store offensive/inappropriate email or documents, breach confidentiality or distribute viruses/virus warnings.
- Use email accounts other than your own, generic/team accounts or those where you have been set up with delegate access.
- Misrepresent the organisation (including via website 'newsgroups', discussion boards or professional 'chat rooms') or enter into contractual agreements.

2 Overview of Organisation responsibilities

The organisation will –

- Reserve the right to routinely monitor system capacity and email volumes.
- Investigate breaches of policy in conjunction with relevant policies.
- Implement and maintain anti-virus software that scans emails, where the local IM&T environment allows.

- Educate users in appropriate use and monitoring that is undertaken.

The organisation may –

- Implement monitoring/blocking software that automatically checks content of email for inappropriate items, such as images, software etc.
- Provide access to a user's email account to their line manager where there is justified need (i.e. period of leave).

The organisation will not –

- Monitor the activity of individuals without consent, unless there is a justified reason identified either by routine monitoring or concerns raised by others.
- Investigate email use for purposes other than gaining access to business communications, monitoring standards of service and training, preventing and investigating crime and identifying unauthorised use of systems.

General items of note:

- Email has the same legal status as a letter and is admissible as evidence.
- Emails can be disclosed in response to a request under the Freedom of Information Act (2000).
- No email system (including policy and processes) is 100% secure. Privacy and security of any personal information you may send is not guaranteed. BrisDoc owns the email facilities and reserves the right to access any document, provided there is a legal justification for the access.
- Inappropriate use (either offensive use, excessive personal use or both) may result in suspension/removal of email access and potential disciplinary action.

3. Using email for business purposes

Email is an acceptable method of communication for healthcare-related business, but it must be used in a way that protects confidentiality and complies with legal and organisational standards.

General Principles

- Always assess whether it is necessary to include identifiable information. If it can be avoided, do so.
- Use the **minimum amount of information** required for the purpose.
- If regular transfers of sensitive data are needed, a **risk assessment** must be completed with support from the Information Governance Lead, SIRO, or Caldicott Guardian.

Sending Identifiable Patient or Sensitive Staff Data

Outside the NHS:

- Do not send identifiable or sensitive data over the internet without additional security measures.

- Use password protection for documents and share the password separately (e.g. by phone or separate email).

Within the NHS:

- Use **NHSMail** for secure communication between NHS users. It provides encryption and is recommended by the BMA and Connecting for Health.
- NHSMail is available to all patient-facing staff at BrisDoc. Corporate staff may have limited access.
- Staff who regularly send patient data should be set up on NHSMail, even if it is not their default email system.
- Ensure recipients are also NHSMail users (addresses ending in @nhs.net).
- **Do not auto-forward** NHSMail messages to non-NHS addresses.

Occasional Transfers of Sensitive Data

If NHSMail is not suitable due to infrequent use, follow these guidelines:

- **Urgent file transfer**: Email the file with password protection and share the password separately.
- **Short messages without attachments**: Prefer phone calls. Avoid leaving voicemail messages that could be overheard.
- **Non-urgent file transfer**: Use encrypted USB or external drives sent via Special Delivery, marked confidential. Share the password upon receipt.

Additional Guidance

- For highly sensitive data (e.g. Sexual Health, Mental Health), consult your Information Governance Lead or Caldicott Guardian.
- Only send data to named individuals with a legitimate need to know.
- Limit the data to what is strictly necessary—avoid sending extra “just in case”.
- Mark emails as **‘Confidential’** in both the subject line and message properties.
- Avoid sending data to individuals who auto-forward their emails.
- Include a note stating that the recipient is responsible for maintaining the confidentiality and security of the data.
- Once received, remove patient data from your inbox and store it appropriately.
- Do not retain patient data in email longer than necessary.
- If others have delegate access to your inbox, consider whether they need to view patient-identifiable information.

4 Timing of personal use and ‘excessive’ use - defined

Limited personal use of email is permitted, provided it does not occur during working hours and is not deemed excessive. Personal email use should be restricted to break or lunch periods.

Excessive use includes activities that place unnecessary strain on the system, such as sending large attachments, which consume storage and slow down email processing. Additionally, clicking on links in personal emails or opening attachments from unknown sources can pose cybersecurity risks, including phishing and malware threats. Always exercise caution and report any suspicious emails to the IT or Information Governance team.

5 Personal gain

You may not use email to make any personal gain, e.g. to run any personal business, or sell items etc. If you wish to advertise such items you should use the Staff Newsletter.

You may use email to respond to such items.

6 Offensive/inappropriate use

You are not permitted to send emails containing material that could be judged to be offensive. Whilst content may not be offensive to you or the recipient(s), there is every chance it will be viewed by others who may find it offensive.

Offensive material would include:

- Abusive, threatening, serves to harass or bully, discriminates, encourages discrimination on racial / ethnic grounds, or grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Obscene, indecent or tasteless images, messages, data or other material.
- Materials that may cause distress, inconvenience or anxiety.
- Material about illegal drugs, computer hacking, militant / extremist behaviour, violence or weapons.

The above list is not exhaustive. BrisDoc retains the right to determine in any investigation what is or is not offensive. If you are in any doubt about whether the content of an email you wish to send could be offensive or not, then do not send it.

7. Auto forwarding:

Email systems have a variety of options to automatically forward messages to others based on a definable set of rules. You must not ‘auto-forward’ patient identifiable or staff sensitive information inappropriately.

8 Use of the BrisDoc name/Contractual arrangements

In any personal emails sent using BrisDoc's facilities, you should ensure it is clear that you are acting in a personal capacity. You may not use email to enter a contractual arrangement on behalf of your employer, nor must you indicate that a potential supplier will be favoured.

9 Retention and deletion of emails

Systems have limited capacity, so you should ensure that you regularly check email and delete messages that are no longer required.

When sending an attachment, if you have the file saved elsewhere (ideally on a networked drive) it is advisable to remove the attachment from your sent items folder otherwise you are doubling the amount of space required to store any document you have created and emailed.

When you receive a message with an attachment, if you need to keep the attachment, you should remove it and store it on a networked drive (in an appropriate folder)

Deletion of messages – retention for Freedom of Information

Most emails (both received and sent) can and should be deleted relatively quickly; however, because of Freedom of Information legislation, certain messages will have to be kept for longer periods as they may be subject to a request and are likely to be disclosable. The following criteria should be used as a guide to determining whether a message should be kept:

If the emails contain discussion/consultation, decisions, or job-related activities then they should be retained.

If the emails are purely 'administrative' then they do not need to be retained. For example, confirmation of attending a meeting

If an email includes an attachment, then if you are the sender, the attachment should be stored elsewhere and can be removed once sent. If you are in receipt of an attachment, you can remove it once you no longer need it, as the sender should be storing it elsewhere. Only delete the email and attachment together, if you do not need to keep the email as well.

The period of retention will depend on the email. The Department of Health Records Management code of practice sets out retention periods for a variety of documents. Key periods relating to emails are listed below:

Emails about projects or initiatives: For those with budgets over £100,000 – 6 years on completion. Those of budgets less than £100,000 – 2 years on completion. For this category only key emails, such as discussions and decisions, where there is no other record, such as minutes, need be retained with other project documentation.

Formal correspondence – such as complaints, 10 years from completion. In such circumstances it is probably best to print emails and include in the appropriate file for the required period.

Patient information – should be printed and stored in the patient record and then removed from the email system.

Emails where you give advice, state a view or make a decision in a professional capacity, that isn't related to a project/initiative, such as responding to a query or relates to operational business, should be kept for 2 years after the matter is settled.

Ensure that retention guidance aligns with NHS Digital's latest **Records Management Code of Practice**. Ask your Information Governance lead for help if necessary

10 Attachments (including those that are, or may contain viruses)

You should avoid sending large attachments, if possible, especially to multiple email addresses as this causes congestion and storage space problems.

You should periodically 'purge' your 'sent' items of attachments, provided you are sure that the original is safely stored elsewhere (network drive, encrypted memory stick/external hard drive)

If you receive attachments that contain 'offensive material', contact your Information Governance Lead who will advise whether the email should be deleted. Whilst deletion should be the course of action in most cases, it may just be the case that deletion removes evidence of another user's misconduct that is important to disciplinary action or in extreme cases legal proceedings.

11 Other email systems

You may access 'personal' email services (e.g. Hotmail or similar) within the boundaries of limited personal use defined above. BrisDoc cannot however guarantee the privacy of staff accessing these facilities from work, as temporary files, Internet page history records are often automatically kept by PCs.

Personal email accounts can NEVER ever be used for BrisDoc-related work.

12 Responsibilities of the Organisation

Monitoring of emails – investigating breaches of policy

Under the Lawful Business Practice regulations (Oct 2000), BrisDoc can lawfully intercept emails for the following purposes:

Gaining routine access to business communications,

Monitoring standards of service and training,

Preventing or investigating crime,

Unauthorised use of systems.

BrisDoc's policy is that the email system will be routinely monitored to ensure that the system is working efficiently and capacity is available.

BrisDoc reserves the right to implement monitoring/blocking software that automatically scans content of emails. If such items are implemented, the rules used to scan content will be determined in conjunction with the Human Resources department.

Individual users will not be monitored without their consent, unless routine monitoring activity/software indicates an issue that requires further investigation or a member of staff raises concerns about a user with a senior manager or the Human Resources department.

Where an issue or concern is raised, the decision about accessing emails without consent will be taken by a senior manager in conjunction with the Human Resources department. The decision will be based on the suspected severity of the issue and whether evidence of misuse is at risk by informing/consenting the suspected user. A formal record of the decision will be made

via 'BrisDoc's incident reporting methods. All monitoring activities will be done proportionately with respect to an individual's right to privacy.

When an investigation is determined as necessary (with or without consent), the Head of Business Information & projects will arrange for a suitably qualified computer forensic investigator to secure the relevant IT equipment.

Any investigation required because of monitoring or identified by other means (e.g. reports from other staff members) will be conducted in line with the organisation's appropriate Human Resources policy, which will give users opportunity to explain actions or challenge results.

All training on the use of e-mail will detail that monitoring can take place and that required investigations can be carried out.

13. Virus Control

The organisation's IT department will ensure that every PC capable of sending/receiving email is fully covered by virus protecting software. They will also ensure that it is regularly updated in accordance with supplier recommendations.

14. Training and Awareness

To ensure safe, lawful, and effective use of email and third-party data sharing, BrisDoc is committed to providing ongoing training and awareness for all staff.

Mandatory Training

- All staff must complete Information Governance training annually, which includes modules on email use, data protection, and secure communication.
- New starters must complete this training as part of their induction programme before accessing email systems.

Awareness and Updates

- Policy updates and reminders will be communicated via:
    - Staff newsletters
    - Intranet announcements
    - Team briefings
- Staff are encouraged to seek clarification from their Line Manager, SIRO or Caldicott Guardian if unsure about any aspect of email or data sharing practices.

Support and Resources

- The IT and Information Governance teams are available to provide ad hoc support and refresher sessions where needed.

Appendix - Change Control

Date	Reviewed and amended by	Revision details	Issue number
Mar-2010	D Douis	Sent for review by IG leads	1
Nov-2010	D Douis	Updates from review	2
Aug-2011	E Jany	Amended departmental procedures + table of contents	3
Nov-2011	DL	Review of Doc, Tidy Up email and faxing sections addition of 3rd Party sharing section.	4
Jul-2012	DL	Review comments CB	4.1
Oct-2012	DL	Merging of GPSU and BRI OOH processes	4.2
Oct-2013	DL	Review in light of new organisation structure. Addition of How Compliance is accessed	4.3
Nov-2013	DL	Review amends after GW review	4.4
Jan-2014	DL	Signed off by NG after review	4.4
Jan-2015	DL	Review in light of new organisation structure.	4.5
Feb-2016	SP	Reviewed / minor amendments	5
Feb-2017	DL	Annual Review	5.1
Mar-2019	SP	Annual review / Fax audit process updated	5.2
Mar-2021	DL	Annual Review	5.3
Mar-2023	DL	Annual Review removal of fax element as no longer used. Changed name of document	5.4
Marc-25	DL	Annual Review on change of SIRO and DPO review	5.5
Jul-25	DL	Rewrite section 3 to make easier to read add section 14	5.6