BrisDoc Patient care by people who care

NHS

Email and third party data sharing operational

Version:	Owner:	Created:
5.5	Deb Lowndes (Programme and Service Director)	1st March 2010
Published:	**Approving Director:**	**Next Review**
07/04/2025	Nigel Gazzard (Managing Director)	07/07/2025

Contents

Document Purpose

This document sets operational guidance for email, faxing 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 above and should be contacted if you are in doubt.

In the event of equipment failure for any reason, staff should refer to the service business continuity plan.

A summary of this document is also available for staff; please refer to the 'Guidance for all staff, volunteers and contractors on handling personal information' leaflet as part of staff induction.

EMAIL

1.1 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 Service Manager for approval and guidance.

Make limited personal use of email during break periods (Lunch/coffee etc).

You must not -

Send identifiable patient data or sensitive data on staff outside the NHS without contacting the Information Governance Lead or Caldicott Guardian for your team 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.

1.2 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.

1.3 Using email for business purposes – including identifiable patient data or sensitive staff data

You may use email as a method of communication for healthcare business. You are legally required to maintain confidentiality of information:

First consider if there is a need to include identifying details – if not, do not include them, always use the minimum information necessary. Communication method is then less critical from a security perspective. If you are looking to set up a regular transfer of sensitive data, a risk assessment should be undertaken, which the Information Governance Lead or Caldicott Guardian for your team will help facilitate.

Identifiable patient data or sensitive staff data –

Outside the NHS:

Must not be sent over the Internet without additional security e.g. password protecting the document,

Within the NHS:

The recommended method for sending identifiable patient data or sensitive staff data is from one NHSMail user to another NHSMail user, as it features encryption (as recommended by BMA and 'Connecting for Health'). NHSMail is not currently in common usage but staff wishing to regularly send patient data via email should be set up to use the system, even though they may not transfer to using NHSMail as their 'default' email solution. They must ensure that the recipients are also users of the NHSMail system (email ends 'nhs.net') Staff using NHSMail for patient data should not auto-forward to any other email address.

Staff not currently using NHSMail, who do not need to send identifiable patient data or sensitive staff data regularly, need to consider which is the most secure method for transfer. If they are not likely to send data more than once every few months, then NHSMail may not be suitable. Below is guidance relating to situations likely to arise. Users should follow this, unless there is good reason not to:

Sending a file of data, required urgently by one or more people – use email, but set a password to access the attached file and communicate it to recipients via a separate message (or via phone). Passwords can be set in the 'Save as' menu. Please ask a manager if you are unsure how to do this.

Sending a short message about a patient(s) where there is no file to attach – best option is a phone call, but be wary of leaving answer phone messages that could be heard by others.

Sending a file of data that is not urgently required, but the recipients require it electronically – password protect the file (as above), send on encrypted data stick or external hard drive via 'Special Delivery' post to named individuals (marked private and confidential), get them to call on receipt to have the password.

General guidance:

If sending extremely sensitive information (Sexual Health, Mental health etc) – please seek support for your method from the Information Governance Lead or Caldicott Guardian for your team.

Only send to named individuals who need to know.

Only send the data, which is needed for the purpose it is being sent. Do not send more, "just in case" you think the recipient needs it.

Mark the message as 'confidential' in the subject as well as in the message properties.

Do not send to individuals who you know forward their emails to other email addresses (potentially outside the NHS).

Include a note to say that the receiver of patient identifiable data is responsible for the security and confidentiality of that data and should not pass it on to anyone else via any method that does not have a justified 'need to know'.

When in receipt of patient data, remove it from your email as soon as possible and file it appropriately, either electronically or on paper.

Do not keep patient data on email for any longer than necessary.

If you allow 'delegate' access to other people to your inbox, consider whether they need to see any patient identifiable data you receive.

1.4 Timing of personal use and 'excessive' use - defined

You can use email for personal use, provided that it isn't during work time or could be considered 'excessive' based on any of the following criteria:

You may use email for personal use during your break or lunch periods. Excessive use includes sending large attachments as this takes up system space and takes time to send. Discuss with your Information Governance Lead or Caldicott Guardian if you are unsure.

1.5 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.

1.6 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.

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.

1.8 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 into a contractual arrangement on behalf of your employer, nor must you indicate that a potential supplier will be favoured.

1.9 Retention and deletion of emails

Storage advice:

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 subject of 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.

Further information can be found in the Department of Health Records Management code of practice. Ask your Information Governance lead for help if necessary.

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

You should avoid sending large attachments, if at all 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.

1.11 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.

Responsibilities of the Organisation

2.1 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 as a result 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.

2.2 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.

2.3 Guidance on using E-mail

Some handy tips on when to use email:

Email should be seen as an additional and complementary communication technology to phone/fax/mail, not as an all-encompassing replacement. Users have differing attitudes to email and will respond (or not) in different ways.

For messages you need to know were sent and received (noting a read receipt only indicates a message was opened, not necessarily read, understood and acted upon). However read receipts should not be routinely requested as this increases email traffic volumes. Not all systems will generate read receipts.

For distribution of information to a large group of people at the same time. However, the sending of large documents or to large distribution lists (especially internal to an organisation) uses up large amounts of disc storage space. It may be best to publish large documents on Intranets/Websites (provided you are happy with who can access them) and send a link to the document via email.

When replying to messages sent to lots of email addresses, only send your response to those that need it, not necessarily all the previous recipients.

Do not count on users reading their email every day. Urgent messages like 'I cannot make the meeting' are best communicated by phone in the first instance, and only sent by email as a backup.

Only use the 'High importance' level indicator on messages that warrant it.

2.4 Confidential/Person identifiable data over email (See policy section 4.4)

Email is not specifically suited to confidential communication as many users leave computers switched on, but unattended. This is the same as leaving a piece of paper on the desk. Other users may also set up delegates or 'auto-forwarding' rules you may not be aware of.

Responding to patient email correspondence – Patients may initiate correspondence via email. You have no way of knowing whether the patient allows access to their email to other people, or how many copies of emails are left on internet servers 'en route' and accessible by unknown individuals. By making contact via email, the patient has implicitly consented to email communication, however as a safeguard you should consider whether an email response is appropriate, and if it is limit the data within it as far as possible, ideally just to an acknowledgement (perhaps for repeat prescription requests etc). For example in a website you may have 'email for repeat prescriptions' or a web-based form, if you intend to send any response (acknowledgement etc) then advertise this in the service. That way any patient who chooses to use it is aware that a response will be sent to the email address they provide.

Other advice

Do not include personal details in any 'out of office' message. Think whether you wish to indicate that you are on holiday. Burglars use mass mailing software and online directories to target empty properties.

THIRD PARTY DATA SHARING

4.1. Background

To securely manage and use data appropriately within BrisDoc it is necessary to identify and risk assess inbound and outbound data flows and to identify all data stores. Having completed the risk assessment, if action is required it should be actioned promptly by the appropriate Service Manager.

4.2 Purpose of this section

The purpose of this section is to provide the necessary guidance to enable the Flow Mapping and Information Asset Register Spreadsheet and associated risk assessment to be completed.

What is an information flow?

The following means of transferring data should be mapped.	Whilst clearly there are security issues relating to other types of data transfer the following should be **excluded** from a data mapping exercise.
✓ Email ✓ Fax ✓ Post/ Courier – hard-copy or electronic media ✓ Text Message	× Phone call × Staff members taking information from A to B internally

✓ Electronic Transfer	× Accessing a system × Accessing a shared drive Security awareness and training for these types of transfer should be managed separately.

Which information flows should be mapped?

✓ Person-identifiable information that • Flows between departments • Flows in/out of organisation *Includes manual/digital flows relating to original and back up/copy data.*	× Non person-identifiable flows × Flows within departments × Patient case notes supporting active care provision × Automated flows between systems

What is meant by person-identifiable?

✓ Contains person name and/or other items of data that could singly or compositely identify the person to whom it relates. NB This includes staff as well as patient data.

4.3 Frequently Asked Questions

Why Is Data Mapping important?

It will help you to understand how data is transferred from and to your organisation and to ensure that measures are in force to ensure that data is secure in transit and that it reaches its destination promptly and safely.

What do you mean by data mapping?

This is the process of documenting the flow of information from one physical location to another and the method by which it "flows". Data flows may be by: E mail, fax, post/courier, text or portable electronic or removable media.

What do you mean by portable electronic or removable media?

This includes tapes, floppy discs, Laptop & handheld computers, Optical discs - DVD & CD-ROM, solid state memory cards, memory sticks and pen drives.

What should I consider as "key areas" for mapping data flows?

Those areas of an organisation which have a high number of inbound and/or outbound person identifiable data flows e.g. an A&E department.

Do I have to map all data flows into and out of the organisation? This would be a mammoth task?

You only need to map routine flows of information that contain sensitive or person identifiable data. Bulk data flows, in particular should be mapped. Ad hoc activities need to be addressed through clear policies, procedures and training.

Would an annual transfer of data be classed as routine, or should this relate more to the frequency of transfer?

Routine flows are those that you know take place on a regular basis – so yes. The frequency of the flow does not really matter.

What do you mean by "sensitive information"? Can you give examples?

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community. This is wider than, but includes, data defined as sensitive under the Data Protection Act 1998.

In addition to personal and clinical information, financial and security information is also likely to be deemed "sensitive".

What do you mean by "personal information?"

This is also referred to as "personal identifiable information" and relates to information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Is "personal identifiable data" the same as "patient identifiable data?"

Personal identifiable data can relate to information held about any individual, not just patients. It may therefore include information about staff, contractors, visitors and members of the public not just patients.

The guidance on data mapping talks about identifying "at risk" flows. What do you means by this?

These are information flows which are not sent to a secure destination, or which are not protected from being intercepted on the way to their destination. Risks are identified so that appropriate action can be taken to secure the data flow.

We often discuss patient information over the telephone; do such calls have to be "mapped" as part of the data mapping exercise?

No. Mapping can only be carried out on tangible information flows and where physical evidence of the information exists. If telephone calls are recorded or discussions transcribed to tapes etc which are then routinely sent to different locations, these will count as data flows. Telephone security is clearly very important but must be addressed through policies, procedures and staff training.

Should I include patient case notes when mapping data flows?

No. Patient case notes can be excluded from data mapping unless there are instances where these are routinely sent outside of the organisation in bulk. e.g. for off-site archiving or GP registration process. Keeping case notes secure is clearly very important but needs to be addressed through policies, procedures and staff training.

Can you explain what is meant by "bulk data"?

Bulk data is defined informally as person identifiable data relating to 51 or more individuals.

Can I ignore data flows that involve the transfer of fewer than 50 records?

No. This figure was provided as a guide only for the immediate action required of Trusts prior to Christmas 2007 though it may help to prioritise work. However, prioritisation should also consider the impact of losing data e.g. the loss of a lower number of highly sensitive records is likely to have a greater impact than the loss of greater number of less sensitive records.

I currently transfer bulk data for clinical audit using DAHNO and LUCADO. Are these systems secure?

These flows should be included in your data flow mapping. However these National systems have been set up to facilitate transfer of information for clinical audit. Both systems encrypt data and, therefore, if used in accordance with the defined and established process, should be secure.

What is the current recommended standard for encryption?

The currently approved cryptographic algorithms for encryption are 3DES, AES (FIPS 197), Blowfish and should be used at the recommended 256bit strength. These algorithms and bit strength are readily available within a range of commercially available off the shelf security products and services. The use of freeware or shareware that does not benefit from independent security evaluation or that fails to comply with these standards should be avoided.

We use NHSmail. Is this secure?

NHSmail is the email and directory service designed specifically for NHS staff, which can be accessed via www.nhs.net. It is the only BMA and Department of Health approved email service for securely exchanging clinical data between NHS organisations but needs to be used by both sender and recipient. You will need to ensure sensitive or personal data is encrypted if it is not sent from and to NHSmail accounts.

1. Tables

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
07/04/2025	JB	Extended as with DPO for review.	5.5