BrisDoc Patient care by people who care

NHS

Data Protection, Confidentiality & Disclosure Policy

Version:	Owner:	Created:
4.6	Deb Lowndes (Head of Business Information and Projects)	1st October 2008
Published:	**Approving Director:**	**Next Review**
17/04/2025	Rhys Hancock (Director of Nursing, AHPs and Governance)	17/04/2027

Contents

Audience

This information is aimed at all BrisDoc employees and contracted individuals or anyone working in or around BrisDoc.

Rationale

All parts of the NHS need to establish working practices that effectively deliver the patient confidentiality. This is required by law, ethics and policy.

BrisDoc is committed to the delivery of a first-class confidential service. This means ensuring that all patient information is processed fairly, lawfully and as transparently as possible so that the public:

- understand the reasons for processing personal information.
- give their consent for the disclosure and use of their personal information.
- gain trust in the way BrisDoc handles information and.
- understand their rights to access information held about them.

Patient identifiable information

Patient identifiable information relates to:

- patient's name, address, full post code, date of birth.
- pictures, photographs, videos, audiotapes or other images of patients.
- NHS number and local patient identifiable codes.
- anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

Why is information confidential?

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician / call handler to clinician).

Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence, and they have the legitimate expectation that staff will respect their privacy and act appropriately.

In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that BrisDoc provides, and is seen to provide, a confidential service.

Patient's health records are made by the health service to support that patient's healthcare. This information must not be disclosed to others without explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. Anonymised information is not confidential and may be used with few constraints.

Anonymised information

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymised information requires the removal of name, address, full post code and any other detail or combination of details that might support identification.

Information after death; is it confidential?

When an individual has died, the information relating to that individual confidential and the right of confidentiality passes to the estate of the deceased individual. The Access to Health Records Act 1990 permits access to the records of deceased by the personal representatives and those with a claim arising from the death of the individual concerned. This right of access is negated however if the individual concerned requested that a note denying access be included within the record prior to death (this might be part of a formal advance directive).

Providing a confidential service

The Confidentiality Model

The model outlines the requirements that must be met to provide patients with a confidential service.

Record holders must inform patients of the intended use of their information, give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be ongoing to aid the improvement of a confidential service. The four main requirements are:

- **PROTECT** - look after the patient's information.
- **INFORM** - ensure that patients are aware of how their information is used.
- **PROVIDE CHOICE** - allow patients to decide whether their information can be disclosed or used in particular ways.
- **IMPROVE** - always look for better ways to protect, inform, and provide choice.

Protecting patient information

Patients' health information and their interests must be protected through a number of measures:

- Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality.
- Recording patient information accurately and consistently.
- Keeping patient information private.
- Keeping patient information physically secure.
- Disclosing and using information with appropriate care.

Informing patients effectively

Patients must be made aware that the information they give may be recorded, may be shared to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided.

In order to inform patients properly, BrisDoc must:

- check where practicable that information leaflets on patient confidentiality and information disclosure are available, have been read, and understood.
- make clear to patients when information is recorded, or health records are accessed.
- make clear to patients when they are or will be disclosing information.
- check that patients are aware of the choices available to them in respect of how their information may be disclosed and used.
- check that patients have no concerns or queries about how their information is disclosed and used.
- answer any queries personally or direct the patient to others who can answer their questions or other sources of information.
- respect the rights of patients and facilitate them in exercising their right to have access to their health records.

It is important to recognize the different communication needs of patients. While some may read leaflets when waiting for treatment, others may be disinclined or unable to do so (through disability, illiteracy, cultural issues or language difficulties). Difficulty in communicating does not remove the obligation to help people understand.

Providing choice to patients

Patients have different needs and values - this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another - just because something does not appear to be sensitive does not mean that it is not important to an individual patient in their particular circumstances.

Staff must:

- ask patients before using their personal information in ways that do not directly contribute to or support the delivery of their care.
- respect patients' decisions to restrict the disclosure or use of information, except where exceptional circumstances apply.
- communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to or restrict the disclosure of information.

Legal considerations

There are a range of statutory provisions that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. Legal requirements and permissions are continually being added to however, so up to date details can be found on the
Department of Health website at

https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

However, there are four main areas of law which constrain the use and disclosure of confidential personal health information.

Common Law of Confidentiality

This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that information confided should not

be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.

UK General Data Protection Regulation (UK GDPR) – Governs the processing of personal data, ensuring legal, fair, and transparent use.

Data Protection Act 2018 (DPA 2018) – Supplements UK GDPR, setting additional provisions for healthcare data, including exemptions and rights.

Human Rights Act 1998 (HRA98)

This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records.

Administrative Law

Administrative law governs the actions of public authorities to ensure that they operate within their lawful powers. In other words, the authority must possess the power to carry out what it intends to do and is particularly relevant to the issue of patient consent.

In the public interest / to protect the public

Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service.

Whoever authorises disclosure must make a record of any such circumstances, so that there is clear evidence of the reasoning used and the circumstances prevailing. Disclosures in the public interest should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision-making process and the advice sought is in the interest of both staff and the organisations they work within.

Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. Where this is not forthcoming, the individual should be told of any decision to disclose against his/her wishes. This will not be possible in certain circumstances, e.g. where the likelihood of a violent response is significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

Each case must be considered on its merits. Decisions will sometimes be finely balanced, and staff may find it difficult to make a judgement. It may be necessary to seek legal or other specialist advice.

Record keeping best practice.
Patient records should:

Be factual, consistent and accurate.

- ☐ Be written as soon as possible after the event has occurred.
- ☐ Be written clearly and legibly and in such a manner that they can't be erased.
- ☐ Be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be seen clearly.
- ☐ Be accurately dated, timed and signed or otherwise identified with the name of the author being printed alongside the first entry.
- ☐ Be readable on any photocopies.
- ☐ Be written, wherever applicable with the involvement of the patient or carer.
- ☐ Be clear, unambiguous (preferably concise) and written in terms that the patient can understand. Abbreviations if used should follow common conventions.
- ☐ Be consecutive.
- ☐ (For electronic records) use standard coding techniques and protocols.
- ☐ Be written to be compliant with the Race Relations Act and the Disciplinary Discrimination Act.

Be relevant and useful.

- ☐ Identify problems that have happened, and the actions taken to rectify them.
- ☐ Provide evidence of the care planned, the decisions made, the care delivered, and the information shared.
- ☐ Provide evidence of actions agreed with the patient (including consent to treatment and / or consent to disclose information.
- ☐ Include medical observations, examinations, tests, diagnoses, prognoses, prescriptions and other treatments.
- ☐ Include relevant disclosures by the patient – pertinent to understanding cause or effecting cure / treatment.
- ☐ Include facts presented to the patient.
- ☐ Include correspondence from the patient or other parties or made to other parties.

Records should NOT include.

- ☐ Unnecessary abbreviations or jargon.
- ☐ Meaningless phrases, irrelevant speculation or offensive subjective statements.
- ☐ Irrelevant personal opinions regarding the patient.

Keeping patient information physically and electronically secure

Staff should not leave portable computers, medical notes or files in unattended cars or in easily accessible areas. Ideally, store all files and portable equipment under lock and key when not actually being used. Staff should not normally take patient records home, and where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed. Please refer to BrisDoc's protocol on Information security available on the intranet.

Cybersecurity and Data Protection

BrisDoc recognises the increasing threat of cyber risks, including phishing, ransomware, and unauthorised access to patient data. To safeguard confidential information, all staff must adhere to BrisDoc's Cybersecurity Policy and the NHS Data Security and Protection Toolkit. Key measures include:

- Using strong passwords and multi-factor authentication (MFA) where applicable.
- Ensuring regular software updates and patch management to mitigate vulnerabilities.
- Avoiding unauthorised data transfers via personal devices or unsecured networks.
- Reporting suspected data breaches or phishing attempts immediately to the Information Governance Lead or IT security team.

In the event of a cybersecurity incident, BrisDoc will follow the Incident Response Plan, ensuring timely containment, investigation, and reporting to the Information Commissioner's Office (ICO) where required. Staff are required to complete annual cybersecurity awareness training to maintain compliance with evolving threats.

Disclosing information with appropriate care

Follow any established information sharing protocols available within BrisDoc.

Staff must follow the principles within this code of practice when sharing information.

Identify enquirers, so that information is only shared with the right people. Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information.

Ensure that appropriate standards are applied in respect of e-mails, faxes and surface mail. Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be.

Guidance is available on the Department of Health website.

Confidentially NHS Code of Practice
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

Share the minimum necessary to provide safe care or satisfy other purposes. This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties) and is likely to constitute a breach of confidence.

The Caldicott principles should be followed-

The Caldicott principles

- **Justify the purpose(s)** - Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
- **Don't use patient-identifiable information unless it is absolutely necessary** - Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
- **Use the minimum necessary patient-identifiable information** - Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
- **Access to patient-identifiable information should be on a strict need-to-know basis** - Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
- **Everyone with access to patient-identifiable information should be aware of their responsibilities** - Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical co-owners - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **Understand and comply with the law** – Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
- **The duty to share information can be as important as the duty to protect patient confidentiality -** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.
- **Inform patients and service users about how their confidential information is used -** A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this.

Improve wherever possible

BrisDoc's confidentiality procedures should be regularly reviewed and the principles in this document adhered to.

Staff must:

- be aware of the basic requirements and where support and further information are available be encouraged to seek out training and guidance to develop a confidential service. Staff must work within both the spirit of this code of practice, and within any locally produced guidelines, protocols and procedures, and be able to demonstrate that they are making every reasonable effort to comply with relevant standards.
- If staff identify breaches or risk of breaches, then they must raise these concerns with their line manager or other appropriate colleagues, e.g. the local Information Governance Lead. Staff must be encouraged and supported by management to report organisational systems

or procedures that need modification. Staff must be made aware of local procedures for reporting where breaches of confidentiality or abuses of patient data are taking place.

Consent Issues

Competence to consent

Seeking consent may be difficult, either because patients' disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object).

- In the former case, extra care must be taken to ensure that information is provided in a suitable format or language that is accessible (e.g. providing large print or Braille versions of leaflets for those with reading difficulties) and to check that it has been understood.
- In the latter case, it will be important to check for a clear and unambiguous signal of what is desired by the patient, and to confirm that the interpretation of that signal is correct by repeating back the apparent choice.

Failure to support those with disabilities could be an offence under the Disability Discrimination Act 1995 and may prevent consent from being gained. Support for communicating with patients having specific disabilities can be obtained from a range of agencies, e.g.

- Royal National Institute for the Blind
- Royal National Institute for the Deaf
- Disability Rights Commission - https://www.drc.org.uk/
- Speakability / Stroke Association - https://www.stroke.org.uk/what-is-stroke/what-is-aphasia

Children and young people

Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to make decisions about the use and disclosure of information they have provided in confidence (e.g. they may be receiving treatment or counselling about which they do not want their parents to know).

However, where a competent young person or child is refusing treatment for a life-threatening condition, the duty of care would require confidentiality to be breached to the extent of informing those with parental responsibility for the child who might then be able to provide the necessary consent to the treatment.

In other cases, consent should be sought from a person with parental responsibility if such a person is available. It is important to check that persons have proper authority (as parents or guardians). Ideally, there should be notes within the child's file as to any unusual arrangements.

Where patients are unable to give consent

If a patient is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the health professionals concerned must take decisions about the use of information. This needs to take into account the patient's best interests and any previously expressed wishes and be informed by the views of relatives or carers as to the likely wishes of the patient. If a patient has made his or her preferences about information disclosures known in advance, this should be respected.

Sometimes it may not be practicable to locate or contact an individual to gain consent. If this is well evidenced and documented and anonymised data is not suitable, the threshold for disclosure in the public interest may be lessened where the likelihood of detriment to the

individual concerned is minimal. Where explicit consent cannot be gained and the public interest does not justify breaching confidentiality, then support would be needed under Section 60 of the Health and Social Care Act 2001

Where the patient is incapacitated and unable to consent, information should only be disclosed in the patient's best interests, and then only as much information as is needed to support their care. This might, however, cause unnecessary suffering to the patient's relatives, which could in turn cause distress to the patient when he or she later learned of the situation. Each situation must be judged on its merits, and great care taken to avoid breaching confidentiality or creating difficulties for the patient. Decisions to disclose and the justification for disclosing should be noted in the patient's records. Focusing on the future and care needs rather than past records will normally help avoid inappropriate disclosures.

Such circumstances will usually arise when a patient has been unable to give informed consent to treatment, and provided the patient has not objected, this may justify the disclosure of some information with relatives in order to better understand the patient's likely wishes. There may also be occasions where information needs to be shared with carers to assess the impact of disclosures to the patient him or herself. Such occasions are rare and justifiable only in the best interests of the patient.

Patients are often asked to indicate the person they would like to be involved in decisions about their care should they become incapacitated. This will normally, but not always, be the 'next of kin'. It should be made clear that limited information will be shared with that person, provided the patient does not object. This gives patients the opportunity to agree to disclosures or to choose to limit disclosure, if they so wish.

Explicit consent

When seeking explicit consent from patients, the approach must be to provide:

- honest, clear, objective information about information uses and their choices - this information may be multi-layered, allowing patients to seek as much detail as they require.
- an opportunity for patients to talk to someone they can trust and of whom they can ask questions.
- reasonable time (and privacy) to reach decisions.
- support and explanations about any form that they may be required to sign.
- a choice as to whether to be contacted in the future about further uses, and how such contacts should be made; and
- evidence that consent has been given, either by noting this within a patient's health record or by including a consent form signed by the patient.

The information provided must cover:

- a basic explanation of what information is recorded and why, and what further uses may be made of it.
- a description of the benefits that may result from the proposed use or disclosure of the information.
- how the information and its future uses will be protected and assured, including how long the information is likely to be retained, and under what circumstances it will be destroyed.
- any outcomes, implications, or risks, if consent is withheld (this must be honest, clear, and objective - it must not be or appear to be coercive in any way); and

- an explanation that any consent can be withdrawn in the future (including any difficulties in withdrawing information that has already been shared).
- The information provided must allow for disabilities, illiteracy, diverse cultural conditions and language differences.

The right to withhold or withdraw consent

Patients do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment.

There are a number of things to consider if this circumstance arises:

- The concerns of the patient must be clearly established and attempts made to establish whether there is a technical or procedural way of satisfying the concerns without unduly compromising care.
- The options for providing an alternative form of care or to provide care through alternative arrangements must be explored.
- Decisions about the options that might be offered to the patient have to balance the risks, staff time and other costs attached to each alternative that might be offered against the risk to the patient of not providing healthcare.

Every effort must be made to find a satisfactory solution. The development of technical measures that support patient choice is a key element of work to determine the standards for electronic integrated care records. Careful documentation of the decision-making process and the choices made by the patient must be included within the patient's record.

Change Register

Date	Version	Author	Change Details
Oct-08	First Draft	D Douis	
Jun-10	Vn 2	D Douis	Sign-ff KR
Jun-11	Vn 3	D Douis	Reviewed, revised review date added
Apr-12	Vn 3.1	DL	Minor formatting changes, text in a table, bullets misaligned
Sept-12	Vn 3.2	DL	Renamed doc to 'Data Protection, Confidentiality & Disclosure Policy' to include relevant sections to meet IG Toolkit requirements
Oct-12	Vn 3.3	DL	Final Version after NG Approval
Oct-14	Vn 4.0	SP	Version reviewed – No amendments
Oct-16	Vn 4.1	DL	Version reviewed – No amendments
Oct - 18	Vn 4.2	SP	DPA 1998 Replaced with DPA 2018. Updated web addresses
Oct-2020	Vn 4.3	DL	Version reviewed – No amendments
Jan 2023	Vn 4.4	DL	Annual Review
March-2025	Vn 4.6	DL	Annual review on change of SIRO with DPO review.