BrisDoc Patient care by people who care

NHS

Monitoring Access to Patient Confidential Information

Version:	Owner:	Created:
2.0	Deb Lowndes (Head of Information and Projects)	1st October 2012
Published:	**Approving Director:**	**Next Review**
25th October 2023	Nigel Gazzard (Managing Director)	1st January 2025

Contents

1. Introduction

The purpose of this document the detail the confidentiality audit procedures that apply within BrisDoc's Out of Hours Service.

2. Objectives of this Procedure

BrisDoc has a number of mechanisms in place to manage and safeguard patient confidentiality.

This document will establish appropriate confidentiality audit procedures to monitor access to confidential patient information. This work forms part of BrisDocs overall Information Governance assurance framework and meets requirements within:

- the NHS Care Record Guarantee - Individuals' rights regarding the sharing of their personal information are supported by the NHS Care Record Guarantee, which sets out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.
- the NHS Data Protection Security Toolkit
- the NHS Confidentiality Code of Conduct

3. Target Audience

This document will be brought to the attention of all staff to raise awareness of the audit and monitoring programme.

4. Scope of the Audits

For the purposes of this procedure, confidential patient information is defined as any information about a patient which would allow that patient to be identified.

All work areas within BrisDoc, which process (handle) confidential patient information will be subject to the confidentiality audit procedures.

Access to both electronic and manual confidential patient information will be audited. Audits across all the BrisDoc's Out of Hours sites will be undertaken and this will help to capture any inconsistencies in practices.

4.1 What the Audits will look for

- Staff awareness of BrisDocs policies and guidelines concerning confidentiality
- Appropriate communications with patients
- Availability of patient information leaflets and notices
- Appropriate recording and/or use of consent forms
- Appropriate use of smartcards
- Appropriate allocation of access rights to clinical systems
- Appropriate patient and staff access to physical areas
- Storage of and access to filed hard copy patient notes and information
- Security of post handling areas
- Security of confidential fax handling

- Security of recorded telecommunications and message books
- Appropriate use and security of the telephone in open areas
- Storage of patient information in public areas e.g. consulting rooms, reception

5. Scope of the Audit Team

The Audit Team will provide the following deliverables

- A nominated lead responsible for implementation
- Detailed audit procedures and auditor specifications
- Trained auditors for the process to be followed
- Planned and implemented audit programme
- Record audit outcomes
- Audit reports and recommendations for the IG Board
- Support with action plans to address any areas requiring review
- Reports to the Caldicott Guardian/IG Board concerning any identified breaches

6. Responsibilities and input

- The ISM will lead on maintaining this document and on ensuring implementation of the audit programme
- The IG Team will support the ISM in the audit activities and any required follow up actions
- The Registration Authority team will provide monitoring reports on smartcard usage, including access to summary care records.
- The Information Security Manager will perform the “Privacy Officer” role, receiving alerts concerning access to restricted electronic records. The SIRO will act as deputy privacy officer in his/her absence.
- The IG Board will incorporate any further training requirements into the IG training programme.
- The Risk Manager, Caldicott Guardian and Senior Information Risk Owner will receive any incident reports as appropriate.
- The Information asset owners will identify their information users, verify their identity, log them in the overarching information asset register, and assign appropriate levels of access, and carry out regular review.

7. Accountability

The outcomes of the audit team’s work will be reviewed by the IG Board.

8. Audit methods and facilities to be utilised

1. Notified audit visits with structured questionnaires
2. Spot checks to random work areas
3. Interviews with staff using structured questionnaires
4. Clinical system usage reporting facilities
5. Registration Authority (smartcard usage) enhanced reporting facilities
6. Regular staff knowledge and understanding surveys
7. Results from the IG toolkit training needs analysis
8. Investigation of reports to the Caldicott Guardian / Caldicott log.

9. Frequency of Audits

For audits involving site visits and staff interviews, BrisDoc will ask 5 questions to 5 staff in all locations, to be repeated twice a year. Questions will be randomly selected from the list in Appendix 1. RA reporting will be done twice a year.

10. Recording the results of the audits and Outcomes

Audit results will be collected on a standard template and then distributed for review/discussion and action at the IG Board.

11. Action planning to rectify areas of concern

The IG Board will ensure that action plans are compiled and implemented to rectify any issues identified from the audits. This will include coordinating the review of relevant policy and procedures and amending the IG training programme as appropriate.

12. Identified incidents of breaches of Confidentiality

Where breaches or risks of breaches in patient confidentiality are identified from the audits, matters will be reported and investigated through BrisDocs Incident reporting procedure. They will also be logged in the Caldicott Log to be reviewed by the Information Governance Board.

Investigations will be carried out by the service are IG Lead where the breach occurred and any correct actions agreed and implemented.

13. Communications

The audit programme will be carried out in an open and transparent manner. The audit procedures and implementation programme will be communicated to management and staff.

14. Staff Disciplinary Procedures

Where appropriate, identified breaches in good practice may be referred to the Human Resources Department, to implement disciplinary proceedings as appropriate.

Appendix 1 - Audit Questions (Correct answers highlighted)

1. Where would you find the BrisDocs IG policies and procedures?

a) Intranet b) memory stick in base c) both

2 What is the principle NHS staff guide concerning patient confidentiality?

a) Code of Confidentiality b) Faxing guidelines c) FOI Act

3. How often should you complete mandatory IG training?

a) every 2 years b) every six months c) annually

4. If you have direct contact with patients should you be explaining and/or should posters/information leaflets be available as to why you are collecting information about them and what you will do with it?

a) yes b) no c) don't know

5. What do you do if you are unable to answer a complex query about how BrisDocs uses patient information?

a) refer to the relevant procedure b) ask my line manager

c) refer to the IG Team d) a and c above

6. Who would you refer patients to concerning a request for access to records

a) Their doctor b) The Governance Team/Practice Manager

c) the IT Team

7. If you lose or find a smartcard you should

a) report this to your Line Manager Immediately who will contact the Registration Authority

b) Cut the card up and throw it away

c) Keep it in your desk in case the owner comes looking for it.

8. It is acceptable to share smartcards because

a) It saves having to keep logging into the system

b) Because you can still do your job if you forget or lose your card

c) Smartcards must never be shared with anyone.

9. Before sharing patient information, wherever possible, it should be:

a) anonymised, b) encrypted c) deleted

10. Any new information assets containing patient information should be:

a) declared to the responsible information asset owner

b) recorded in the information asset register

c) risk assessed to mitigate any information security issues

d) all of the above

11. If you discover a breach of confidentiality you should:

a) Reprimand the offender b) tell the patient c) report via the learning event portal

12. In addition to facilitating hot desking, the clear desk policy helps to ensure:

a) that the cleaner can access the desk tops

b) that patient information is secured when not in use

c) that you get a good reputation for being tidy

13. Is it acceptable for staff to discuss patients where other people can hear?

a) Yes b) No

14. What is the leaflet that informs patients about information use?

a) How we handle your information

b) patient information

c) information and you

15. You should never connect personal equipment into your laptop or PC because

a) risk of transferring viruses b) the network will crash c) a and b

16. The Caldicott Guardian is

a) Rhys Hancock b) Kathy Ryan c) Nigel Gazzard

3. Tables

Date	Reviewed and amended by	Revision details	Issue number
31/08/2012	DL	DRAFT	1.0 DRAFT
12/10/12	DL	Review of first draft	1.1
28/2/14	DL	Review for use of intranet tool to perform the audit	1.2
Feb 15	DL	Reviewed change CG reference	1.3
Deb 17	DL	Annual Review	1.4
Nov 18	DL	GDPR Review	1.5
Oct-2020	DL	Version reviewed – No amendments	1.6