MONITORING ACCESS TO PATIENT CONFIDENTIAL INFORMATION POLICY

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

Contents

DOCUMENT CONTROL

Document Storage

Location: P:\Ops Team\Central Policies & Procedures - Development - Word Docs\IG - IGSoc - GDPR Policies\IG-32 - Monitoring Access to Patient Confidential Information V1.11.docx

Version Control Log

(Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V1.9	April 2022	S Barnes	Under review
V1.10	July 2022	S Barnes	Reviewed, no changes
V1.11	Sept 2023	J Carey	Reviewed, minor changes

Approval

Version	Name	Position	Signature	Approved Date
V1.4	IGSG	IG Steering Group		09 March 2017
V1.5	IGSG	IG Steering Group		14 March 2018
V1.6	Badger Executive	Executive Team		25 July 2019

Glossary

Term	Description
IGSG	Information Governance Steering Group
SIRO	Senior Information Risk Officer
PO	Privacy Officer
PII	Personally Identifiable Information
SCD	Special Category Data

1 INTRODUCTION

Badger already has a comprehensive range of control mechanisms in place to manage and safeguard patient confidentiality.

This document will establish appropriate confidentiality audit procedures to monitor access to confidential patient information throughout Badger. This work forms part of Badger's overall assurance framework and meets requirements within:

- NHS Digital Data Security and Protection Toolkit
- NHS Digital Registration Authority Governance
- HSCIC Code of Practice on Confidential Information – December 2014
- Records Management Code of Practice for Health and Social Care August 2021

2 TARGET AUDIENCE

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

3 SCOPE OF THE AUDITS

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

All work areas within Badger, which process (handle) PII will be subject to the confidentiality audit procedures.

Access to both electronic and manual confidential patient information will be audited. Audits across all Badger's sites will be undertaken, and this will help to capture any inconsistencies in practices.

3.1 What the Audits will look for

- Staff awareness of Badger 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., Urgent treatment centres and cars

4 SCOPE OF THE AUDIT TEAM

The Audit Team will provide the following deliverables.

- A nominated lead responsible officer for implementation
- Detailed audit procedures and auditor specifications
- Trained/Briefed auditors
- Planned and implemented audit programme
- Database to record audit outcomes
- Audit reports and recommendations for the IG Steering Group
- Support with action plans to address any areas requiring review
- Reports to the Caldicott Guardian concerning any identified breaches.

5 RESPONSIBILITIES AND INPUT

- The Information Governance (IG) Lead will lead on maintaining this document and on ensuring implementation of the audit programme
- The Clinical Governance team will provide expert advice on audit training and audit design.
- The Operations team member with the responsibility of Registration Authority team will provide monitoring reports on smartcard usage, including access to summary care records.
- The Information Security Officer will perform the "Privacy Officer" role, receiving automated alerts concerning access to restricted electronic records.
- The IG Lead will incorporate any further training requirements into the IG training programme.
- The CEO, Caldicott Guardian and Senior Information Risk Owner will receive any incident reports as appropriate.
- The Operations Department 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.

6 ACCOUNTABILITY

The IG Lead will report to the Caldicott Guardian, the Senior Information Risk Owner and Badger's Information Governance Steering Group (IGSG), on behalf of the audit team.

7 TRAINING FOR THE NOMINATED AUDITORS

The audit team will receive in-house training from Badger's IG Lead/SIRO and Caldicott Guardian on how to design and carry out the audits and how to manage the results of the audits.

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 DS&P training needs analysis
8. Investigation of reports to the Caldicott Guardian / Caldicott log.

The "Privacy Officer" function will act on behalf of the Caldicott Guardian. The Privacy Officer will monitor data accessed and make judgements on each case, based on whether the user had a legitimate relationship with the patient i.e. whether the access was justified or illegal. Where inappropriate behaviour is suspected, further investigations will follow, possibly resulting in incident reports in accordance with the Badger IG-08 SUI Procedure. This will include notifying the Caldicott Guardian, SIRO and IG Lead.

9 FREQUENCY OF AUDITS

Audits will be conducted at least annually and will consist of site visits where staff interviews will take place. Questions will be randomly selected from the list in appendix A, At least 10 questions will be asked in each interview, and questions will be varied between different staff.

10 RECORDING THE RESULTS OF THE AUDITS

Audit results will be collected on a standard template and then recorded in a database for future reporting and analysis.

11 AUDIT OUTCOME REPORTING

Results from the audits will be collated and a report compiled. The report will be submitted to the Information Governance Steering Group (IGSG). The group will highlight any areas requiring further development and make recommendations concerning any corrective actions required.

12 ACTION PLANNING TO RECTIFY AREAS OF CONCERN

The IG Lead will lead on ensuring 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.

13 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 Badger's Incident reporting procedure. They will also be logged in the Caldicott Log by the IG Lead and reviewed by the Information Governance Steering Group.

Investigations will be carried out by the Departmental manager where the breach occurred, and any corrective actions agreed and implemented in line with Badger's current policies and procedures.

14 COMMUNICATIONS

The audit programme will be carried out in an open and transparent manner. The audit procedures and implementation programme will be communicated, where appropriate, to management and staff through the Adastra comms tab. The documentation will be made readily available via Badger's normal communication channels (Adastra, Bulletins, etc).

15 STAFF DISCIPLINARY PROCEDURES

Where appropriate, identified breaches in good practice may be referred to the Departmental Manager, to implement disciplinary proceedings.

16 REVIEW OF THIS PROCEDURE

This procedure will be reviewed by Badger's Information Governance Steering Group every 2 years.

17 APPENDIX A – SAMPLE AUDIT QUESTIONS

IG Lead and IGSG will format the questionnaire prior to the audit session. Below are sample questions to show the scope covered by the audit.

No	Question	Options	
1	Where would you find Badger's IG policies and procedures?	a) Adastra b) Information leaflet and Publication scheme c) Control Centre d) All	
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 attend mandatory DS&P refresher training?	a) Every 2 years b) Every six months c) Annually	
4	If you have direct contact with patients should you be explaining 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 Badger uses patient information?	a) Refer to the relevant procedure b) Ask my line manager c) Refer to the IG Lead d) a and c above	
6	How should you record patient consent to share information?	a) On the relevant file b) By memory c) Recording is not necessary	
7	Who would you refer patients to concerning a request for access to records?	a) Their Doctor b) Your Manager c) The IG Lead	
8	If you lose or find a smartcard you should	a) report this to the Registration Authority Immediately b) cut the card up and throw it away c) keep it in your desk in case the owner comes looking for it.	
9	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.	
10	Before sharing patient information, wherever possible, it should be:	a) anonymised, b) encrypted c) deleted	

No	Question	Options	
11	In accordance with the Information Lifecycle Management Procedure, documents should include	a) version control b) author c) date d) all the above	
12	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	
13	If you discover a breach of confidence you should:	a) reprimand the offender b) tell the patient c) submit an incident form	
14	In addition to facilitating hot desking, the clear desk policy helps to ensure:	a) that the cleaner can access the desktops b) that patient information is secured when not in use c) that you get a good reputation for being tidy	
15	Telephone messages containing patient information should be received by	a) secure voice mail b) insecure answer phone c) nearest passer by	
16	Is it acceptable for staff to discuss patients where other people can hear?	a) Yes b) No	
17	What is a safe haven	a) A special fax machine b) A secure repository for patient information c) A refuge for homeless people	
18	What is a Fair Processing Notice?	a) Explains how personal information is used and shared b) States that information is not collected c) Protects the organisation from being sued	
19	What is the name of Badger 's fair processing notice?	a) How we Handle Your Personal Information b) Data Processing c) Fair choice	
20	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	