Standard Operating Procedure

AUDIT AND ACCEPTABLE USE

SETTING Trust-wide

FOR STAFF For all staff who use Trust information systems and for staff who will undertake audits of these systems

ISSUE This SOP explains the acceptable use of Trust information systems and the procedure of proactive audits to discover any unauthorised access to confidential information.

Standard Operating Procedure (SOP)

Introduction

Access to Trust information systems is granted to staff members in order to carry out their role. Staff members should only use these systems to access records of patients they are involved in the direct care or administration of. Accessing records of patients who you do not need to do as part of your job, including those of friends and family members, as well as your own records, is unauthorised access.

All NHS bodies are required to have confidentiality audit procedures in place that determine whether confidentiality has been breached or has been put at risk through deliberate misuse of systems, or as a result of weak or poorly designed access controls (Data Security & Protection Toolkit Requirement Assertion 1.5.2).

Definitions

Access – Searching for or viewing a record.

Access Controls – A set of rules on an information system that limit access to information.

Audit – A formal process to monitor account usage.

Confidentiality – Maintaining the privacy associated with health information.

Information System – A digital programme that allows access to patient, staff member, or other members of the public's electronic record.

Unauthorised Access – Searching, viewing, altering or deleting a record that you have no valid reason to as part of your employment.

Roles and Responsibilities

Senior Information Risk Owner (SIRO)

- Executive lead for the implementation of the Information Governance Policy and takes overall responsibility for the management of information risk.

Information Governance Team (IGT)

- To advise SMs on audit procedures

- To advise on actions following unauthorised access discovery
- Report instances of unauthorised access to Information Risk Management Group

Human Resources Business Partners (HRBP)

- To maintain awareness of investigations within their division

Human Resources Information Systems (HRIS)

- Provide a list of staff, their line managers and their divisions to IG fortnightly

Employee Services (ES)

- To assist line managers with their investigations
- To feedback any further actions taken to Information Governance

Line Managers (LM)

- To investigate audit activity
- To escalate unauthorised access to Employee Services
- To notify the IG of where access was legitimate

System Managers (SM)

- To develop audit procedures with the advice of IG
- To conduct quarterly audits of their systems

All Staff (AS)

- To only access the records that they need to as part of their employment

Procedure

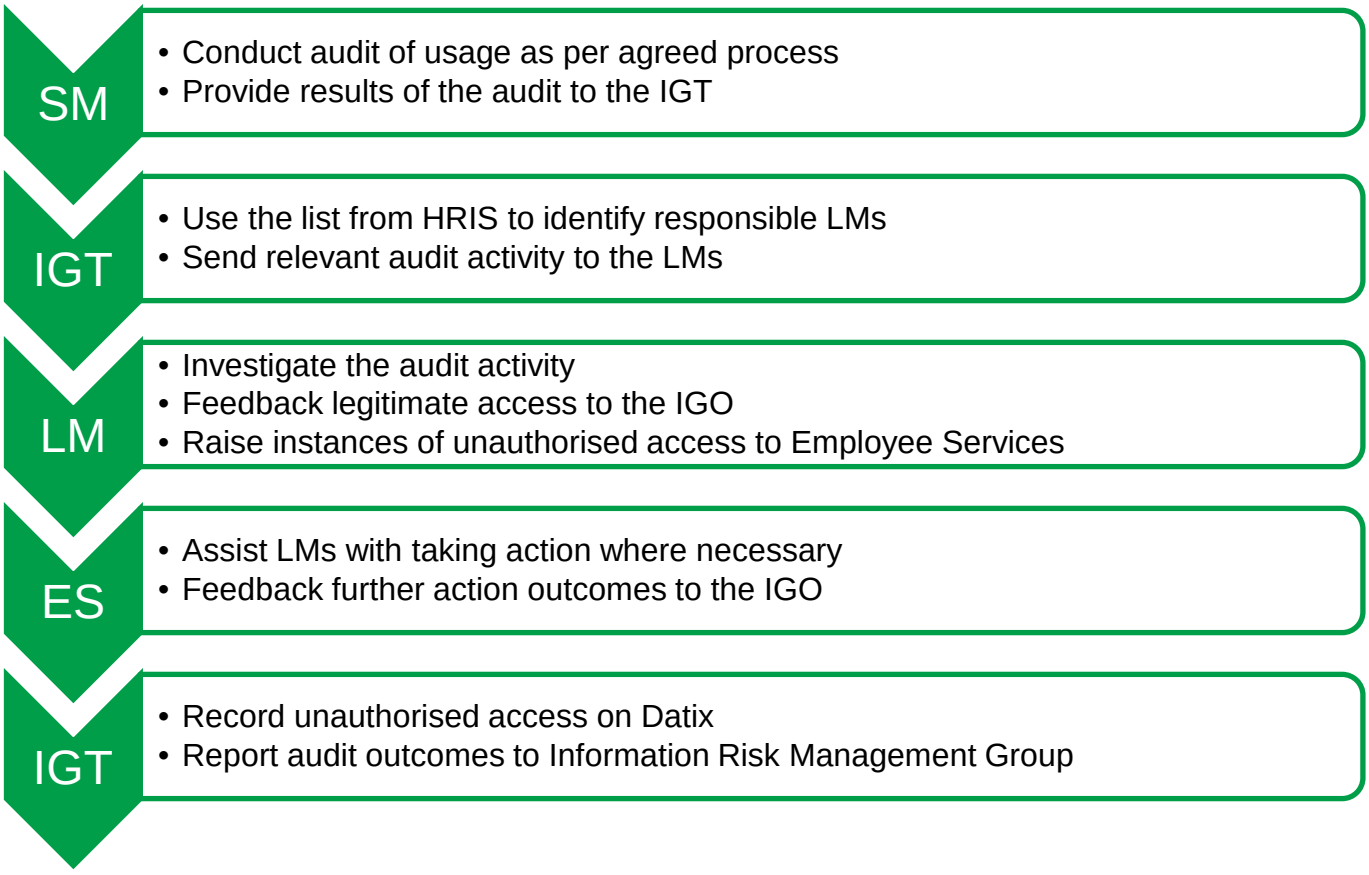

Table A

REFERENCES	None
RELATED DOCUMENTS AND PAGES	Information Governance Policy Staff Conduct Policy Information Security Policy
AUTHORISING BODY	Information Risk Management Group
SAFETY	None
QUERIES AND CONTACT	Information Governance InformationGovernance@UHBristol.nhs.uk, x23701/x23794