Falkland Islands Government

Department of Health and Social Services

Guidance for conducting an Audit on Access to Electronic Patient Records

Author(s): Healthcare Governance Manager/Data System Administrator

Issue Date: **February 2023**

Version No: **v.0.3**

Status: **Active**

Review Date: **February 2025**

Amendment History

Version	Status	Summary of Changes	Date of Issue
v.0.3	**Active**	**Changes Made – Document now active**	**February 2023**
v.0.2	Draft	Submitted to SMT for discussion. Prior to activating the document, it was identified that: Title changed to 'Guidance' and inclusion of the word 'Access' Inclusion of previous Laboratory system ASET with regard to auditability Social Services systems omitted from this guidance. Request for Audit of deceased patient records included	February 2023

Contents

1. Introduction

Information provided by patients to healthcare professionals is confidential in law.
It is considered as personal data and it is protected. Occasions arise when the confidentiality of data held electronically is questioned, usually as a result of a complaint or concern raised by a service user. It must be emphasised that allegations of data breaches are taken seriously and action will be taken.

In order to provide assurance that access to personal confidential data is gained only by those individuals that have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis. This will be achieved by putting in place arrangements for both proactive (3 monthly) and reactive auditing of access by the Data System Administrator.

The KEMH commits to providing information to service users on who has accessed their records (if requested) and taking action against individuals who access information inappropriately. However, it must be noted that if a period of over one year has elapsed, it may be difficult to conduct a meaningful investigation due to the fact that the member of staff may no longer be employed.

Actual or potential breaches of confidentiality should be reported immediately to the Healthcare Governance Manager and by logging this as an incident on Q-Pulse, in order that the incident can be assessed for severity and action taken to prevent further breaches.

This document indicates the steps which should be taken to investigate where a query has been raised that electronic data held may have been accessed inappropriately.

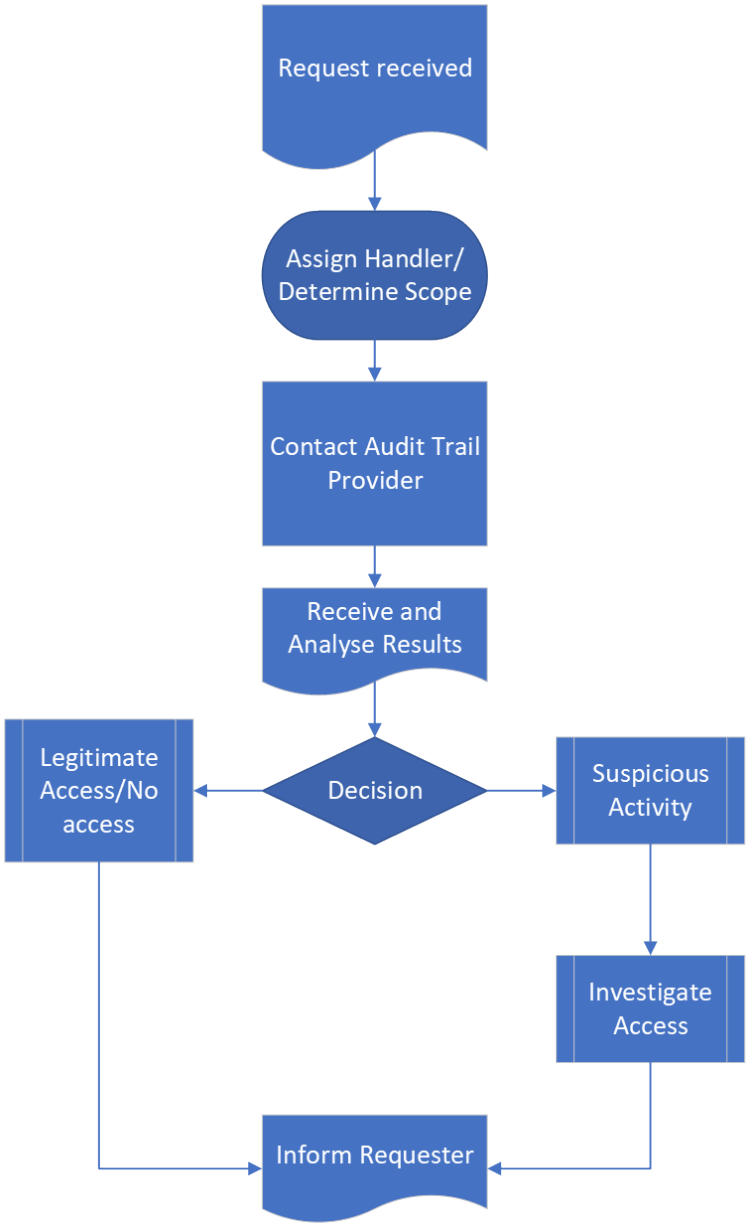
Should unauthorised access to personal confidential data be gained by any individual or if information is disclosed to unauthorised recipients, this will be dealt with in accordance with the requirements of the FIG Management Code and potentially the Code of Public Conduct and may result in referring the matter to the RFIP.

Caldicott principles should be adhered to at all times, with only the relevant information being shared regarding the need for the audit.

1.1 Glossary of terms

Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. • An internal audit is conducted by the organisation itself, or by an external party on its behalf.
Audit Scope	Extent and boundaries of an audit.
Terms of Reference	Used to define the scope of an audit, the terms of reference, ToR, should establish the focus and objectives of the audit, the audit timetable (including reporting), and a summary of staff to be engaged in the work, along with the audit tools and techniques that will be used. The terms of reference should be agreed prior to the audit starting.
Documented Evidence	Information required to be controlled and maintained by an organisation and the medium on which it is contained.
Personal Data	Protected under Data Protection legislation / GDPR, personal data is data relating to an identified or identifiable natural person.

2. The process



2.1. Receive Query

A query (request) may be received through a variety of routes, for example via a complaint, through a police investigation, through a solicitor acting on behalf of client, or the investigation of an audit trail may be volunteered by the KEMH to help allay a service user's concern over confidentiality of their data.

The information required to conduct an investigation is:

- the patients name;
- address;
- date of birth;
- the time period over which the investigation is to take place
- the specific reason for the request

The request may be to investigate if a specific individual has accessed a record, or to identify if an unknown person (to the requester) has accessed a record.

With regard to deceased patients please seek advice from the CMO as Caldicott Guardian.

It must be noted that confidentiality continues after death and it is the deceased personal representative (usually the executor or administrator of their estate) who would be able to request an audit.

2.2. Assign Auditor / Determine Scope

The nature of the query and the way it is received will usually determine who will handle (own) the investigation (i.e. be the point of contact with the patient and co - ordinate internal activity as necessary).

Typically, a query will arise through either a complaint or direct request. If a staff member receives a request from patient such as "How did xx know about my hospital appointment", or "Who has been looking at my records", contact the Healthcare Governance Manager who will handle the query through the complaints process.

The Healthcare Governance Manager (or deputy) will act as the auditor.

The scope of the investigation will depend upon the nature of the query. If the query is about a specific piece of information e.g. "how did xx know about my blood test result", then clearly an audit trail will be required from the pathology system - LabVantage. The same applies to imaging and the head of the specific department may be asked to conduct a separate audit on their electronic data system.

If in doubt about whether a service user has records on a particular system, ask for an audit trail anyway. If the records don't exist the KEMH have fulfilled its duty to investigate thoroughly.

Where multiple systems are involved (see 2.3.) it may be more appropriate to pass the query through to the Healthcare Governance Manager who will co-ordinate the internal activity.

If in any doubt as to what action to take, staff should check with their Line Manager in the first instance. Who, in turn can seek advice from the Hospital Manager or Chief Medical Officer.

2.3. Contact audit trail provider

Healthcare software applications have usually audit trail functionality. The following are the systems where an audit trail is most likely to be required. Systems below are now considered as legacy ones and data quality and it`s availability would vary. Currently in use in KEMH we have:

System	Contact
EMIS PCS	Healthcare Governance Manager/Data System Administrator
IMPAX	Radiographer/Healthcare Governance Manager
LabVantage	Pathology Manager/Clinical Governance Manager

However, we are unable to conduct audits on ASET which has been subsequently replaced by LabVantage as it did not have audit capabilities.

It must be noted that only those systems used within the KEMH are auditable, this guidance is not applicable to those systems used within the Social Services department.

2.4. Receive and investigate the results

Investigation of the audit trail to identify irregularities within any of the above systems will be carried out by the HGM or/with nominated person in the first instance.

However, the results may need cross checking with other systems, for example the LabVantage or Impax system.

Cross checking data is the responsibility of the auditor.

Reactive/Investigation audits may identify evidence of:

- Unauthorised viewing/access to clinical records;
- Failed attempts to access confidential information;
- Repeated attempts to access confidential information;
- Successful access of confidential information by unauthorised staff;
- Evidence of shared login sessions;
- Inappropriate communications with patients/service users;
- Inappropriate recording and/or use of sensitive/patient information;
- Inappropriate allocation of access rights to systems or other data;
- Inappropriate staff access to secure/restricted areas.

The investigation should result in a view that access has been legitimate (or where there is no evidence to support suspicious activity) or suspicion over the access. Suspicion will lead

to a more detailed investigation by Healthcare Governance Manager in conjunction with the member of staff's Line Manager (see 2.6.).

It **does not mean** the access is inappropriate, only that a further investigation needs to take place.

Documented Evidence should be attached to any further investigation.

2.5. Access legitimate

Where the access is legitimate, or no evidence supports inappropriate access, the auditor will write to the service user, outlining the investigation which has taken place (what, over what period) and stating the outcome.

The requester does have the right to a copy of the audit trail if requested. Reasonable effort to assist the requester in interpreting the audit trail must be made.

2.6. Suspicious access

Where the audit trail raises a concern that the activity of a person may not be legitimate, the evidence must be forwarded to the Hospital Manager or Chief Medical Officer, who will review the information received, query if required, and begin an internal investigation with the individual(s) concerned.

In this situation, it is appropriate to inform the requester that an investigation is underway. The name of the individual should normally be withheld during the investigation stage.

If, during the internal investigation process, the individual is found to have unauthorised access to clinical records, then disciplinary action will be taken in accordance with the FIG Management Code. If there is suspicion of criminal activity, then the case will be referred to RFIP for further investigation.

3. Document Retention

All requests and communication on investigations should be retained by the HGM.

(Any documentation which is used in an HR investigation or staff disciplinary will be held a part of the disciplinary process documentation).

4. Awareness of this procedure

Line Managers are responsible for the dissemination of this guidance among current employees.
Newly appointed staff would be made aware of this guidance during the induction process.

5. Contact

Should you require any further details regarding interpretation of this guideline please contact the Healthcare Governance Manager or Data System Administrator.