NHS
Counter Fraud Authority

Confidentiality Audit Procedure

October 2019

FCG-IG-CP-016 Version: 2.0

NHS fraud.
Spot it. Report it.
Together we stop it.

Version control

Version	Name	Date	Comment
V.1.0	Finance & Corporate Governance	August 2018	Annual Review August 2019
V.2.0	Finance & Corporate Governance	October 2019	Annual Review October 2020

Table of Contents

1. Introduction

1.1 The purpose of this document is to set out established and appropriate confidentiality audit procedures, to monitor access to confidential person-identifiable information throughout the NHS Counter Fraud Authority (NHSCFA). This policy document forms part of the NHSCFA's overall governance and assurance framework to meet the requirements within:

- the Department of Health's Data Security and Protection Toolkit; and
- the NHS Confidentiality Code of Conduct

1.2 This policy covers all information systems purchased, developed and managed by/or on behalf of the NHSCFA and any individual directly employed or otherwise by the organisation.

2. Scope of audits

2.1 For the purposes of this policy, confidential person-identifiable information is defined as any information about a person which would allow that person to be identified either directly or indirectly.

2.2 All work areas within the NHSCFA which processes confidential person-identifiable information will be subject to a confidentiality audit.

2.3 Access to both electronic and manual confidential person-identifiable information are liable to be audited. Audits may be undertaken across all the NHSCFA sites, which will help to ensure any inconsistencies in practices are captured. The Board may agree 'terms of reference' for an exercise to be undertaken internally by the Governance & Assurance team or agree for an exercise to be undertaken by an external auditor.

2.4 Decision as to the scope and location of the audit will be agreed between the Audit Lead, the relevant Senior Management Team Lead and the Information Governance Lead.

3. Audit approach

3.1 What the audits will look for:

- staff awareness of NHSCFA policies and guidelines concerning confidentiality
- appropriate recording of consent (where applicable)
- appropriate allocation of access rights to systems

- appropriate staff access to physical areas
- storage of and access to filed hard copy person-identifiable notes and information
- security of post handling areas (where applicable)
- storage of person-identifiable information in open/public areas
- security of recorded telecommunications and messages

3.2 Audit methods used may include horizontal or vertical audit of whole or partial areas of the business. The evidence or information gathered and/or examined may include (although this is not an exhaustive list):

- notified audit visits with structured questionnaires
- spot checks to random work areas
- interviews with staff using structured questionnaires
- annual staff knowledge via e-learning pathways
- results from the IG toolkit training needs analysis
- investigation of reports/or submissions to the Caldicott Guardian

3.3 The audit Sponsor will agree how the following deliverables will be provided:

- a nominated lead responsible officer for implementation
- detailed audit procedures and auditor specifications
- trained auditors
- a planned and implemented audit programme
- a spreadsheet/database to record audit outcomes
- audit report/ recommendations for the Board and the Information Governance Lead
- support with action plans to address any areas requiring review
- reports to the Caldicott Guardian concerning any identified breaches.

3.4 Audit results will be collected on a standard template and kept for future reporting and analysis.

4. Roles and responsibilities

Caldicott Guardian

4.1 It is a requirement for all NHS organisations to appoint a Caldicott Guardian, who must be a senior person within the organisation. The Chief Executive is the NHSCFA's appointed Caldicott Guardian and they have overall responsibility for protecting the confidentiality of people's health and care information and making sure that it is used appropriately.

Information Governance Lead

4.2 The role of the Information Governance Lead is to help ensure the organisation's handling and sharing of personal data is undertaken in a confidential and secure manner, to appropriate ethical, professional and legal standards.

Audit Lead

4.3 The audit lead will ensure the successful design and conduct of the assurance audit.

Auditor Pool

4.4 The pool is comprised of staff, of all grades from across the organisation that have been trained to conduct internal audits under the instruction and guidance of the Senior Governance and Assurance Officer. Where an IG exercise is conducted as part of the wider Governance & Assurance programme, the audit pool may contribute to these exercises.

5. Audit findings

5.1 Results from the audits will be collected on a standard template setting out both findings and recommendations and kept for future reporting and analysis. The report will be submitted to the Information Governance Team, highlighting any areas requiring further development and make recommendations concerning any corrective actions required.

5.2 The Information Governance Lead will ensure that action plans agreed with the Audit Sponsor are compiled with and implemented, to rectify any issues identified from the audit. This will include co-ordinating the review of relevant policy and procedures and suggesting recommended amendments to the staff IG training programme as appropriate.

5.3 All audit recommendations and management responses will be captured and fed into the Board Assurance Framework document; providing the Board and the Audit Risk Committee with a thorough oversight the organisation's operational and strategic risk.

5.4 Where breaches or risks of breaches in person-identifiable confidential information are identified from the audits, matters will be reported and investigated through the

NHSCFA's Service Desk. Where appropriate the Caldicott Guardian will also be notified so that the issue can be entered in the relevant 'Caldicott 'Incident Log', which may be reviewed by the Information Governance Team & IT Security Group.

6. Review of this policy

6.1 This procedure will be reviewed by the Information Governance team on an annual basis as part of a responsive approach to learn lessons and deliver continued improvement.