NHS Counter Fraud Authority

Information Governance Strategy

September 2018

Version 2.0

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

Version control

Version	Name	Date	Comment
V 1.0	Trevor Duplessis	22/01/18	Review May 2018
V 2.0	Trevor Duplessis	September 2018	Update

Table of contents

1. Introduction

1.1 This strategy covers the period 2017-20 and describes the continuing development, implementation and embedding of a robust Information Governance (IG) framework needed for the effective management and protection of NHS Counter Fraud Authority (NHSCFA) information.

1.2 IG describes the approach within which accountability, standards, policies and procedures are developed and implemented, to ensure that all information created, obtained or received by the organisation is held and used appropriately.

1.3 The strategy confirms NHSCFA's commitment to compliance with information rights legislation and confirms our commitment to good practice. It sets out an approach that will deliver all of the essential compliance elements, in a way that also actively enables and supports the delivery of the organisation's corporate objectives and allow it to exploit new and emerging opportunities.

1.4 NHSCFA has a responsibility to manage and protect a wide range of information to ensure that it remains confidential, preserves its integrity and availability. Such information includes:

- information obtained during the course of investigations
- information obtained from individuals raising concerns about fraudulent activity
- information provided by individuals relating to concerns about how their information has been processed
- information obtained during audit processes; and
- information which supports the running of the organisation including records relating to staff

1.5 This approach will allow NHSCFA to further its corporate objectives by being open and transparent about what it does and to be accountable for the actions it takes. It will give confidence to those who provide or share personal identifiable information with us, that their information will be handled and managed appropriately.

2. Scope

2.1 This strategy is applicable to all NHSCFA staff and business units, information systems and records and other information assets of the organisation and includes within its scope:

- the framework of accountability and responsibility for information assets
- information security
- the management of the life cycle by which information is created, received, obtained and disposed.
- the arrangements under which information from third parties is received and used, as well as permitted uses of information disclosed to stakeholder partners.
- efforts to build quality information practice in staff and stakeholders through training and awareness

2.2 This strategy excludes NHSCFA's obligations in relation to the handling of information requests made to the organisation under the General Data Protect Regulation (GDPR), the Data Protection Act 2018 and the Freedom of Information Act 2000.

3. Business plan - Information Governance

3.1 In NHSCFA's plan, as part of its strategic goal to develop and use its intelligence function, to analyse the crime risks across the NHS and wider health group, it is also committed to pursuing the following objectives:

- increase the quantity of fraud reports and actionable intelligence
- develop the central counter-fraud intelligence system hub to enhance the capture, evaluation and management of information
- increase the effectiveness of the organisation's information analytics capability by increasing its information data sets
- enhance the on-line information portal for external stakeholders

3.2 If we are to achieve these objectives NHSCFA must create an environment which ensures that:

- its staff have a high level of awareness of their obligations under information rights legislation and other regulatory requirements and that those obligations are routinely met in practice
- good information handling practice is embedded into the culture and day to day business processes of the organisation, as well as into the design and acquisition of new technologies and system
- information management processes are streamlined and robust, creating a high level of confidence in the quality of its information that supports efficient day to day practice and good decision making; and
- promotes the secure exchange of information with other agencies that we collaborate with to fulfil our objectives.

3.3 This information governance strategy is a clear statement of NHSCFA's commitment to high quality information management and to technical and physical information security good practice. It recognises that investment in information governance supports and contributes to both our corporate objectives and our regulatory responsibilities.

4. Regulatory landscape

4.1 NHSCFA as a data controller will be subject a legal framework, including but not limited to the:

- General Data Protection Regulation (GDPR) and the Data Protection Act 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003

Other related legislative and common law provisions:

- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Common Law duty of confidentiality
- Re-use of Public sector Information Regulations

Related guidance and codes of good practice:

- Cabinet Office's Security Policy Framework
- NHS Digital guidance
- Information Commissioner's Office guidance and standards

Standards:

- ISO 27001 - Information Security Management System
- ISO 15489 - Information and Documentation Records Management (1&2)

5. Information governance aims

5.1 There are three elements to NHSCFA's information governance landscape; information security, data protection and records management. Each element requires policy, process and defined standards. While there are overlaps between the elements, each has its primary focus and together they form a complete information governance discipline. NHSCFA's information governance aims are described below encompassing all of these elements and other important considerations. The achievement of these aims will not only help to deliver essential compliance requirements, but will also enable and support the organisation's core business functions.

Information security

5.2 We have implemented a comprehensive information security management system (ISMS) aligned to the international best practice standard ISO 270001. This will ensure that NHSCFA has robust, proportionate and compliant information security measures in place so that the organisation is protected against threats from unauthorised or unintended access, destruction, disclosure or tampering.

5.3 All business units will work to ensure that information security policies are aligned with operational requirements and find solutions appropriate to NHSFCA's risk appetite. NHSCFA will support its staff by ensuring that information security policies and processes are clear and easy to understand, that help and guidance are available when needed, and by providing appropriate training to minimise the risk of error. NHSCFA will provide an assurance function that sets clear security standards against which all technology developments will be measured.

Collation and use of personal information

5.4 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 set out the requirements and safeguards which must be applied to personal data, to ensure the rights and freedoms of living individuals are not compromised. It is NHSCFA's obligation as a Data Controller to comply with the Regulation and the Act.

5.5 HSCFA will:

- comply with the law in respect of the data it hold about individuals
- hold information securely and confidentially
- obtain information fairly and efficiently
- record information accurately and reliably
- share information appropriately and lawfully; in addition we will promote transparency and openness about how we handle personal information providing confidence to individuals and third parties who pass personal information to us.

Record management

5.6 We will ensure that staff competency in records management is developed and supported by appropriate processes and technologies, to achieve the following benefits:

- information is trusted, authentic and reliable
- information enables high quality decision making with information quality contributing to improved public confidence in NHSCFA
- information handling is compliant and efficient
- information supports and does not hinder collaboration internal or external

Retention/Destruction

5.7 It is essential that all information is not only used, communicated, transferred and stored in a manner that complies with the broader information management and security framework of the NHSCFA; but also ensures that disposal of records is undertaken in accordance with legislation, key guidance and the orgainsation's

Data Handling, Storage Retention & Records Management policy and accompanying data retention schedule.

5.8 Management and staff should be undertaking regular 3 to 6 monthly reviews of the data they hold, to help guard against exposing the organisation to unnecessary and avoidable risk. Any data no longer required for the purposes for which it was obtained, should with the authority of the Information Asset Owner and/or the SIRO, be deleted.

Embedding a compliance culture

5.9 NHSCFA will ensure that its information governance policies are embedded in the day to day operations of the organisation, that they are compliant with relevant legislation, standards and codes of practice, to demonstrate good practice and meet the public interest. The policies are based on a risk management approach that recognises that information has significant value, is commensurate with our stated risk appetite and is aligned with business requirements.

Education and awareness

5.10 NHSCFA will aim to embed a high level of staff and stakeholder awareness of the organisation's governance policy and processes, to help achieve compliance and reduce the risk of avoidable incidents and breaches through error. Fostering a culture of personal responsibility, ownership and commitment to the highest standards of information handling to support and enable our business functions.

Audit and assurance

5.11 NHSCFA will ensure that there are processes in place to check whether information governance policies are being adhered to and measure its effectiveness. The Governance and Assurance team will work with business unit leads and Information Asset Owners (IAOs) to gain feedback about the practical operation of policies and practice.

5.12 NHSCFA will act on this feedback and make appropriate changes where necessary. Governance and Assurance, Information Governance and IAOs will work together to share experience and maximise the opportunities to learn from examples of good practice, both internal and external.

6. Information governance management framework - roles and responsibilities

6.1 We have appropriate structures in place to ensure that there are clear delegated duties, responsibilities, decision-making powers and processes embedded within NHSCFA's operational processes. Roles and responsibilities are described in brief below.

Senior Information Risk Owner (SIRO)

6.2 Richard Hampton is the NHSCFA's SIRO and is a member of the Senior Management Team (SMT). His role is to take ownership of the organisation's information risk policy, act as an advocate for the management of information risk to the SMT and provide written advice having considered the annual governance and assurance report/statement in respect of information risk.

6.3 The SIRO has overall responsibility for understanding how the strategic business goals of the organisation may be impacted by information risks and for sponsoring and promoting information governance policy across the organisation.

Caldicott Guardian

6.4 Sue Frith and Richard Rippin are the NHSCFA's Caldicott Guardians. The Guardian plays a key role in ensuring that NHSCFA and stakeholder organisations satisfy the highest practical standards for handling personal identifiable information; acting as the 'conscience' of the organisation.

6.5 The Caldicott Guardian also has a strategic role alongside the SIRO, to champion information governance requirements and issues across all of the business units as part of the organisation's overall governance framework.

Information Governance Lead

6.6 The Information Governance Lead is responsible for the provision of subject matter expertise to the organisation, in respect of legislative compliance and adhering to best practice in Information Rights, Records/Content Management and Information Security.

Information Asset Owner (IAO)

6.7 IAOs are accountable for the quality of and access to information created, received or obtained by their business area. Additionally IAOs are responsible for identifying, assessing and managing the risk associated with their information assets.

NHSCFA staff

6.8 All NHSCFA staff have a personal responsibility to understand and adhere to the organisation's information governance policies and procedures, applicable to their specific role.

7. Independent assurance

7.1 NHSCFA will have independent, internal and external assurance arrangements in place to ensure compliance with information governance and information security legislation, regulations and good practice.

8. Review cycle

8.1 The implementation of the Information Governance strategy, policy and procedures will ensure that information is more effectively managed within NHSCFA.

8.2 This document will be reviewed at least annually and an action plan developed against the IG toolkit to identify key areas for continuous improvement.