NHS
Counter Fraud Authority

Confidentiality Policy

February 2020

FCG-IG-CP-19: Version 1.0

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

Document control

Document title	Confidentiality Policy
Intent	This is the approved Confidentiality Policy for the NHS Counter Fraud Authority. It is to be maintained by the F&CG Information Governance & Risk Management Lead.
Version	1.0
Document status	Final
Issue date	n/a
Planned Review date	January 2022
Author	Trevor Duplessis
Document Owner	Trevor Duplessis
Reviewed by	Leadership Team/Senior Management Team
Authorised by	Ann Sturgess - Corporate Governance Manager and Board Secretary

Version/change control

Version	Name	Date	Comment
1.0	T Duplessis	07/11/2019	

Table of Contents

1. Introduction

1.1 The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within the NHS Counter Fraud Authority (NHSCFA) and have access to person-identifiable or confidential information (see appendix D). All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

1.2 All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation in the UK - the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018). Confidentiality is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

1.3 It is important that NHSCFA protect and safeguard all person-identifiable information and confidential business information that it gathers, creates, processes and discloses; in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to the public and its stakeholders. This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non-NHS organisations.

1.4 Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth or NHS number.

1.5 Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes NHSCFA confidential business information.

1.6 Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, tablets, mobile phones, digital cameras or even heard by word of mouth. Confidential or personally identifiable information must not be stored on removable media unless it is appropriately encrypted. A summary of Confidentiality Do’s and Don’ts can be found at Appendix A.

1.7 The Legal and NHS Mandated Frameworks for confidentiality which form the key guiding principles of this policy can be found at Appendix B. How to report a breach of this policy and what should be reported can be found at Appendix C. Definitions of confidential information can be found at Appendix D.

2. Scope

2.1 The Board and all staff without exception, fall within the scope of this policy.

3. Roles and Responsibilities

3.1 The Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that NHSCFA policies comply with all legal, statutory and good practice guidance requirements.

3.2 The Caldicott Guardian

A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing by providing advice to professionals and staff.

3.3 Senior Information Risk Owner (SIRO)

Signs off and takes accountability for risk-based decisions and reviews regarding the use, disclosure or processing of confidential data in the operating functions of NHSCFA.

3.4 Data Protection Officer (DPO)

Provides advice to the organisation and its employees on data protection issues which can include confidentiality issues which, where appropriate will be reviewed in collaboration with the Caldicott Guardian as appropriate to ensure the organisation's compliance with data protection law.

3.5 BSA HR

HR are responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate inductions for all staff.

3.6 Senior Manager Team (SMT)

Are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Information Security Incident Reporting Process.

3.7 Corporate Governance Manager & Board Secretary

Has overall responsibility for ensuring the policy is kept up to date, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff to further their understanding of the principles and their application.

3.8 Leadership Team (LT)

Are responsible for ensuring that there are agreed standard operating procedures (SOPs) in place, within their business areas and these are followed by staff.

3.9 All staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003. There is generally a confidentiality clause in contracts of employment and it is mandatory to participate in induction, e-learning and awareness raising sessions carried out to inform and update staff on confidentiality issues.

3.10 Any deliberate breach of confidentiality, inappropriate use of health data, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal and must be reported to an appropriate line manager and via the NHSCFA Information Security Incident reporting process. Where a duty of confidence is broken or breached, civil legal action may be taken against those responsible to secure financial recompense.

3.11 Section 170 (1) of the Data Protection Act 2018 - Unlawful obtaining etc. of personal data, states it is an offence for a person knowingly or recklessly:

a. to obtain or disclose personal data without the consent of the controller

b. to procure the disclosure of personal data to another person without the consent of the controller, or

c. after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

It is important to note that there may be situations where both the organisation and the individual concerned can be held liable.

4. Corporate Level Procedures

4.1 Principles

All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of
- Access to person-identifiable or confidential information must be on a need-to-know basis
- Use of person identifiable or confidential information must be limited to that purpose for which it was acquired
- Recipients of disclosed information must be informed that it is given to them in confidence
- Any decision taken to either disclose or without information, seek consent or rely on another justifiable ground, must be appropriately recorded and documented
- Any concerns about disclosure of information must be discussed with either the Line Manager or the F&GC Information Governance Team.

4.2 NHSCFA is responsible for protecting all the information it holds and must always be able to justify any decision to share information. Person-identifiable information, wherever appropriate, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

4.3 Access to offices and rooms where terminals are present, or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

4.4 All staff should clear their desks at the end of each day. In particular, they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked. Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, removable media, tapes and printouts etc. containing personal data and/or confidential information must not be left lying around but be filed and locked away when not in use. NHSCFA's contract of employment makes clear that every employee is now personally liable to protect the confidentiality of the information they enter, process or encounter. Breaches of confidentiality could

be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal or civil legal action.

4.5 Disclosing Personal/Confidential Information

To ensure that information is only shared with appropriate people in appropriate circumstances, care must be taken to check that we have a legal basis for accessing and disclosing the information and the recipient has a legal basis for receiving it. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

4.6 Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice (https://ico.org.uk/)
- When the information is required by law or under a court order. In this situation staff must in the first instance notify the Information Governance (IG) team. The IG team will if necessary, consult the Caldicott Guardian before advising
- In identifiable form, when it is required for a specific legal purpose, or with the data subject's written consent
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must in the first instance notify the IG team. The IG team will if necessary, consult the Caldicott Guardian before advising.
- For any proposed routine disclosures of personal/confidential information, please consult the NHSCFA's Information Sharing Agreements Policy.

4.7 If staff have any concerns about disclosing information, they must in the first instance raise it with the IG team. The IG team will if necessary, consult the Caldicott Guardian before advising.

4.8 Care must be taken in transferring information to ensure that the method used is the most secure. Data sharing agreements provide a way to formalise arrangements between organisations. For further information on Information Sharing Agreements contact the IG team and/or see the Information Sharing Agreement Policy document.

4.9 Staff must ensure that appropriate standards and safeguards are in place to protect against inappropriate disclosures of confidential personal data. When transferring patient information or other confidential information by email, methods that meet appropriate NHS encryption standards must be used.

4.10 Emails between NHS Mail accounts meet this requirement (nhs.net to nhs.net). Emails between NHS Mail and other secure government domains also meet this requirement (e.g. gov.uk).

4.11 Personally identifiable information and Official-Sensitive information CAN be sent in a standard email so long as the email is classified as 'Official-Sensitive' by the sender. Egress will automatically encrypt the entire email when sent to a non-approved recipient domain thereby negating the need to password-protect attachments. This will remain the position when we migrate to the new Office 365 email system.

4.12 Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry NHSCFA information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents. Please refer to the organisation's Mobile Working Policy.

4.13 The taking home/removal of paper documents that contain person-identifiable or confidential information from NHSCFA premises is discouraged unless considered absolutely necessary. To ensure safety of confidential information staff must always keep them on their person whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

4.14 When working away from NHSCFA locations staff must ensure that their working practice complies with the organisation's policies and procedures. Any electronic removable media must be encrypted as per current practice. Staff must minimise the amount of person-identifiable information that is taken away from NHSCFA premises. If staff need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of NHSCFA buildings.

- Confidential information is kept out of sight whilst being transported and/or kept away from prying eyes whilst being worked on in transit.

4.15 If staff need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car where it could be viewed by a member of the public through a window.

4.16 Staff must NOT forward any person-identifiable or confidential information via email to personal e-mail accounts. Staff must not use or store person-identifiable or confidential information on privately-owned electronic devices.

4.17 Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts and other documents
- Leave a computer terminal unattended and with screen unlocked when logged on to a system where person-identifiable or confidential information can be accessed

4.18 Steps must be taken to ensure physical safety and security of person-identifiable or confidential/sensitive business information held in paper format and on computers. Passwords must be kept secure and must not be disclosed to anyone. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal. This could also constitute an offence under the Computer Misuse Act 1990.

4.19 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose, unless through established self-service mechanisms where such access is permitted (e.g. viewing your ESR record). Under no circumstances should employees access records about their own family, friends or other persons without a legitimate purpose and it being undertaken by an independent third party. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018. When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of NHSCFA.

4.20 Confidentiality audits provide mechanisms that allow all organisations that handle person-identifiable or confidential information to test the processes they have in place to highlight actual or potential confidentiality breaches in their systems and the procedures to evaluate the effectiveness of controls within these systems. This function may be performed by external auditors or internally by the Governance and Assurance (G&A) team through a programme of agreed audits.

5. Distribution and Implementation

5.1 Distribution Plan

This document will be made available to all staff via the intranet site.

5.2 Training Plan

The Organisational Development (OD) Unit's training programme for e-learning, incorporates a training needs analysis for all NHSCFA staff. Based on the findings of that analysis, appropriate training will be provided to staff as necessary.

6. Monitoring

6.1 Compliance with the policies and procedures laid down in this document will be monitored via the Finance & Corporate Governance (F&CG) Unit and may be subject to internal G&A audit or external audit.

6.2 The Information Governance Lead is responsible for the revision and updating of this document on a biennial basis or sooner if the need arises.

7. Associated Documents

7.1 The following documents will provide additional information:

- Acceptable Use Policy
- Records Management (Primary) Policy
- GDPR Data Protection Act Policy
- Information Governance Policy
- Information Security Incident Reporting Policy

- Information Sharing Agreement Policy
- Mobile Working Policy
- Information Security Policy
- Source Protection Policy
- SIT Dissemination Process Standard Operating Procedure
- Information Breach Reporting Policy

Appendix A

Confidentiality Do’s and Don’ts

Do’s

- Safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHSCFA
- Clear your desk at the end of each day, keeping all non-digital records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Switch off computers with access to person-identifiable or business confidential information, or put them into a password protected mode, if you leave your desk.
- Ensure that you cannot be overheard when discussing confidential matters.
- Challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Share only the minimum information necessary to achieve the purpose.
- Transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gov.uk.
- Seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person’s consent and record the decision and any action taken.
- Report any actual or suspected breaches of confidentiality through Service Desk (servicedesk@nhscfa.gsi.gov.uk, Ext: 0207 895 4545, Int: 514 4545) where it will be appropriately triaged.
- Participate in induction, e-learning and awareness raising sessions on confidentiality issues.

Don’ts

- Don’t share passwords or leave them lying around for others to see.
- Don’t share information without the consent of the person to which the information relates, unless there are statutory or common law grounds to do so.

- Don’t use person-identifiable information unless absolutely necessary, anonymise the information wherever possible.

- Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B:

Summary of Legal and NHS Mandated Frameworks

NHSCFA is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of NHSCFA, who may be held personally accountable for any breaches of information security for which they may be held responsible. NHSCFA shall comply with the following legislation and guidance as appropriate:

GDPR and DPA 2018

Regulate the use of “personal data” and sets out six principles to ensure that personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. Accurate and where necessary kept up to date

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Caldicott Report (1997)

Together with the subsequent Caldicott or National Data Guardian reviews recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information

- Don’t use patient identifiable information unless it is absolutely necessary

- Use the minimum necessary patient-identifiable information

- Access to patient-identifiable information should be on a strict need-to-know basis

- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

Article 8 of the Human Rights Act (1998)

Refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990)

Makes it illegal to access data or computer programs without authorisation and establishes four offences:

- Unauthorised access to data or programs held on a computer e.g. to obtain or view information about friends and relatives.
- Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
- Unauthorised acts with intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation; and
- Making, supplying or obtaining articles for use in offences 1-3

The NHS Confidentiality Code of Practice (2003)

Outlines four main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information
- Inform patients how their information is used
- Allow patients to decide whether their information can be shared
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The NHS Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly regarding patients’ rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so
- We ask, and you give us specific permission
- We have to do this by law
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality and
- If we share information without your permission, we will make sure we abide by data protection legislation, the NHS Confidentiality Code of Practice and other national guidelines on best practice.

Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Appendix C

Reporting of Information/IT Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported and triaged through Service Desk (servicedesk@nhscfa.gsi.gov.uk, Ext: 0207 895 4545, Int: 514 4545). Once this has been done staff should report the matter to their line manager.

If staff are unsure whether a particular activity amounts to a breach of an information governance or IT security policy, they should discuss their concerns with their line manager or the Information Governance team. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords
- Unauthorised access to NHSCFA systems either by staff or a third party
- Unauthorised access to person-identifiable information where the member of staff does not require access or have a need to know
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with data protection legislation and the NHS Code of Confidentiality
- Sending person-identifiable or confidential information in a way that breaches confidentiality
- Leaving person-identifiable or confidential information lying around in a public area
- Theft or loss of person-identifiable or confidential information
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing of person-identifiable information in an ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or the Information Governance team should be sought.

Reporting of Breaches

See the organisation’s Information Breach Reporting Policy.

Appendix D

Definitions

The following types (this list is not exhaustive) of information are classed as confidential:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Any data or combination of data and other information, which can indirectly identify the person, will also satisfy the definition.

Confidentiality

A duty of confidence arises where one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

Special categories of personal information (previously known as 'sensitive' personal data) as defined by GDPR and the DPA 2018 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic and Biometric data
- Health data
- Sexual history and/or sexual orientation
- Criminal convictions data

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, these should also be treated with the same degree of care.