NHS
Counter Fraud Authority

Law Enforcement Processing (Data Protection) Policy

August 2019

Version: 1.1- FCG-IG-CP-005

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

Version control

Version	Name	Date	Comment
V.0.1	Finance & Corporate Governance	July 2019	Draft
V.0.2	Finance & Corporate Governance	July 2019	Comment revision
V.1.0	Finance & Corporate Governance	August 2019	Final
V.1.1	Finance & Corporate Governance	September 2019	Minor revision Annual Review September 2020

Table of contents

1. Introduction

1.1 Under the law enforcement processing provisions of the Data Protection Act (DPA) 2018, where a controller, the NHS Counter Fraud Authority (NHSCFA) carries out sensitive processing based on one or more of the specified conditions in Schedule 8 of the Act[1], it must have an appropriate policy document in place.

1.2 The policy must explain the procedures for complying with the data protection principles when relying upon one or more of the conditions set out in Schedule 8 and the organisation's policy for the retention and erasure of personal data for this specific processing. The policy must be retained from the commencement of the sensitive data processing, until at least six months after it has ended and must be made available to the Information Commissioner upon request, without charge.

1.3 This policy explains the special requirements the NHSCFA must meet when processing personal data relating to criminal offences (including the suspected and alleged commission of an offence) and how staff can comply with those requirements while carrying out their work. The policy also satisfies the DPA's requirement for NHSCFA to have in place an 'appropriate policy document' governing such processing.

2. Definitions

2.1 **Anti-fraud organisation** - any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes[2].

2.2 **Data Protection Legislation** - the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), the Data Protection Act 2018 and any accompanying regulations that may apply to the legislation detailed above.

2.3 **Processing** - an operation or set of operations which is performed on person identifiable data or sets of personal data, such as the:

- collection, recording, organisation, structuring or storage
- adaptation or alternation
- retrieval, consultation or use

[1] Conditions for sensitive processing under Part 3

[2] Section 68(8) Serious Crime Act 2007

- disclosure by transmission, dissemination or otherwise making available
- alignment or combination; or
- restriction, erasure or destruction

2.4 **Competent authority** - either a person specified in Schedule 7[3] or any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.

2.5 **Law enforcement purpose** - the prevention, investigation, detection or prosecution of criminal offences (including alleged commission of a criminal offence) or the execution of criminal penalties, including the safeguarding against the prevention of threats to public security.

2.6 **Sensitive data** - in addition to criminal offence data, it also includes the processing of any of the data below, by a competent authority for a law enforcement purpose:

- data revealing racial or ethnic origin, political opinions/affiliations, religious or philosophical beliefs or trade union memberships
- genetic or biometric data for the purpose of uniquely identifying an individual
- health data; or
- data relating to an individual's sexual orientation

3. Scope

3.1 There are potentially three scenarios where NHSCFA may be involved in the processing of personal information for the purpose of preventing and detecting the commission of criminal offences; namely:

- where NHSCFA as a competent authority is performing its statutory function
- where the NHSCFA is involved with, but is not performing its statutory function; and
- where the processing relates to disciplinary actions, regulatory breaches or civil liabilities

3.2 This policy applies to the first of these scenarios. Information processed in relation to the final scenario must be processed in accordance with the NHSCFA's Data Protection (GDPR) Policy.

[3] Data Protection Act 2018

This policy therefore, should inform the activities of ALL NHSCFA staff engaged in law enforcement processing.

3.3 Is NHSCFA a competent authority?

The NHSCFA is competent authority, falling under both of the requisite criteria under section 30 of the DPA 2018, namely:

- as person specified or described in Schedule 7[4] or
- any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes[5]

Processing Activity	Legislative Provisions	NHSCFA Policy
Where NHSCFA is exercising its statutory function as a competent authority	Part 3 of the DPA 2018	Section 5 of this policy
Where NHSCFA is not exercising its statutory function but processing criminal offence data	Parts 1,2 & 3 of Schedule 1 of the DPA 2018 (*by virtue of section 10(4)&(5) and Article 10 GDPR*)	Data Protection (GDPR) Policy
Where information relates to disciplinary actions, civil offences or regulatory breaches	GDPR & Part 2 DPA 2018	Dealing with DPA (Excluding SAR) Request Policy

4. Aims

4.1 The aims of this policy are to:

- ensure that all NHSCFA staff and any third parties processing data on the organisation's behalf are aware of which data protection, legislative provisions apply to the processing they are conducting
- ensure that all NHSCFA staff and any third parties processing data on the organisation's behalf are aware of the data protection principles and lawful conditions that apply in respect of each
- explain the safeguards that NHSCFA has in place to secure compliance with data protection principles and protect the rights and freedoms of data subjects when processing sensitive personal data relating to criminal offences[6]; and

[4] 1. Any United Kingdom government department other than a non-ministerial government department

[5] The NHS Counter Fraud Authority (Establishment, Constitution and Staff and Other Transfer Provisions) Order 2017

[6] Section 42 of 2018 Act

- identify the responsibilities of NHSCFA staff and any third parties in complying with the law that applies in respect of each strand of processing.

5. Law enforcement processing

5.1 The GDPR expressly states that its provisions do not apply to the processing of personal information by a competent authority for law enforcement purposes[7]. EU Directive 2016/680 - the Law Enforcement Directive sets out the standards Member States' own legislation must meet for this type of processing. In the UK this is set out in Part 3 of the DPA 2018.

5.2 Specifically, 'law enforcement processing' captures the processing by a competent authority of criminal offence and criminal penalty data, whether wholly or partly by automated means or where the data forms, or is intended to form part of a filing system.

5.3 Compliance with the data protection principles

Where NHSCFA as a competent authority, processes personal information for a law enforcement purpose, the processing must satisfy the principles below:

- it must be fair and lawful
- purposes of processing must be specified, explicit and legitimate
- personal data must be adequate, relevant and not excessive
- personal data must be accurate and kept up to date
- it should not be kept for longer than necessary; and
- it must be processed in a secure manner.

More on the principles is provided below:

5.3.1 First Principle - fair and lawful processing

Data subjects must be told that their data is being collected, who is collecting it and what we intend to do with it. NHSCFA makes this information available through its privacy notice on its website. A privacy notice must be in place and made available to the subject before any information is obtained from them. Where personal information is not obtained from the subject directly a notice must be provided in each of the scenarios below at the earliest:

[7] Article 2(2)(d)

- at the date of the first communication with them; or otherwise
- if data is to be disclosed to another recipient, before the date of disclosure,
- but in either event, within one month at the latest

However, where a law enforcement purpose would be prejudiced by notifying the data subject of the processing of their data, then an exemption from the above obligations may be applied.

5.3.2 Processing conditions

In addition to being fair and lawful, one of the following conditions in all cases must also be met:

- the data subject has given their consent to the processing, or
- the processing is necessary for the 'performance of a task' carried out by a competent authority for a law enforcement purpose.

5.3.3 Processing conditions (sensitive data)

Processing of sensitive data for a law enforcement purpose will only be lawful if:

- explicit consent has been gained from the subject, or
- the processing is strictly necessary for a law enforcement purpose and meets one of the further conditions outlined in Schedule 8 of the DPA 2018 Act (see Appendix A).

In both cases NHSCFA must have in place an appropriate policy document as required by sections 35(4)&(5) of the DPA Act 2018.

5.3.4 Second principle - processing purpose

Personal data collected for a law enforcement purpose must be specific, explicit and legitimate.

Personal data can be processed for a further purpose, but only where that 'further' processing is not incompatible with the initial processing purpose. To be compliant with this principle the NHSCFA must be authorised by law to process for the further purpose and the processing must be necessary and proportionate to that purpose.

Example:

Information collected for the purpose of an investigation must not be used for the incompatible purpose of sending marketing materials.

However lessons learned from an investigation and/or subsequent successful prosecution could be further used by the organisation to inform prevention initiatives (although the need to use person identifiable information would be the exception) without falling foul of the processing principle.

5.3.5 Third principle - relevancy

The information collected and processed for a law enforcement purpose must be adequate, relevant and not excessive for the purpose it is collected. Only the minimum amount of information necessary to achieve the purpose in question must be processed (i.e. requested, collected or shared).

5.3.6 Fourth principle - accuracy

The personal data must be accurate and kept up to date. Where compatible with the processing purpose inaccurate data must be erased or rectified as soon as it is found to be incorrect.

5.3.7 Intelligence

It is also a requirement of the law, that insofar as possible, personal data based on personal assessment and opinion (including intelligence) be distinguished from that which is based on fact.

5.3.8 Sharing data

Inaccurate, incomplete or out of date information must **not** be shared for any law enforcement purpose. To that end:

- personal data must be verified before being shared
- an assessment of the accuracy, completeness and reliability of the data must be included when data is shared; and
- recipients must be informed if personal data is found to be inaccurate or the sharing unlawful.

5.3.9 Fifth principle - retention

Personal data must be kept for no longer than is necessary to achieve the law enforcement purpose. A suitable retention period must therefore be established to guide periodic reviews of the personal data held[8].

Once the retention period has been exceeded the information must be deleted unless further retention is justified in accordance with the 'Archiving' condition (see Appendix A). Information must not be retained beyond the defined organisational retention period without the reasons being specified and recorded.

5.3.10 **Sixth principle - data security**

Information processed for a law enforcement purpose must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The organisation's Information Security Policy sets out these security requirements.

5.4 Data subjects have the following rights:

- to be informed of our use of their information
- of access to their information
- rectify inaccurate personal information
- to have their information erased (right to be forgotten)
- to restrict how we use their information
- to move their information to a new data controller (where applicable)
- to object how we use their information
- to object to direct marketing
- not to have decisions made about them on the basis of automated decision making; and
- to complain about anything NHSCFA does with their information.

A data subjects rights **may be restricted** in whole or in part where they would conflict with a law enforcement purpose.

[8] Relevant retention periods are detailed in the NHSCFA's Data Retention Schedule

6. Categories of data

6.1 Where possible a distinction between data relating to the categories of individuals must be made, such as:

- suspects
- those convicted of criminal offences
- victims, and
- witnesses

6.2 It should be borne in mind that some individuals could fall within more than one category, such as a 'victim' could also be a 'witness'. We will only categorise the information under Part 3 of the Act **where relevant** to an investigation; any unused data will fall under the general provisions of GDPR (Part 2 of the 2018 Act). Any unused personal data will also be subject to the organisation's retention periods.

7. Safeguards - processing data

7.1 Article 10 of the GDPR requires that Member States provide safeguards for the rights and freedoms of data subjects in any national law they may enact to authorise the processing of personal data relating to criminal convictions and offences.

7.2 For this reason, sub-sections 35(4)((b) & 35(5)(c) of the DPA 2018 requires controllers when processing criminal data to have an appropriate guidance document in place. Section 42 further defines the content of such a policy, in that it should:

- explain how NHSCFA will ensure compliance with the data protection principles described in the paragraphs above,
- explain the NHSCFA's policies as regards the retention and erasure of personal data processed in reliance on a particular condition, giving an indication of how long such personal data is likely to be retained,
- be retained, reviewed and (if appropriate) updated periodically
- be made available to the Information Commissioner on request and without charge

8. Review

8.1 This policy will be reviewed no less than an annually.

Further sensitive processing conditions

Further conditions for processing sensitive data for a law enforcement purpose are detailed in Schedule 8 of the Data Protection Act 2018. The most relevant to NHSCFA are:

Statutory purpose

The processing is necessary for the exercise of a function conferred on a person by an enactment…and is necessary for reasons of substantial public interest.

Legal claims

The processing is necessary for:

- the purpose of, or in connection with, any legal proceedings, including prospective legal proceedings,
- the purpose of obtaining legal advice; or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights

Preventing fraud

The processing (including disclosure) is necessary for the purposes of preventing fraud or a particular kind of fraud, and

- the NHSCFA is acting as a competent authority as a member of an anti-fraud organisation, or
- in accordance with arrangements made by such an organisation.

Archiving

The processing is necessary for

- statistical purposes