NHS
Counter Fraud Authority

Processing Special Category and Criminal Convictions Data Policy

April 2021

FCG-IG-CP-20: Version 2.0

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

Document control

Document title	Processing Special Category and Criminal Convictions Data Policy
Intent	This is the approved Processing Special Category and Criminal Convictions Data Policy for the NHS Counter Fraud Authority. It is to be maintained by the F&CG Information Governance & Risk Management Lead.
Version	2.0
Document status	Approved
Issue date	April 2021
Planned Review date	April 2022
Author	Trevor Duplessis
Document Owner	Trevor Duplessis
Reviewed by	Trevor Duplessis
Authorised by	Ann Sturgess - Corporate Governance Manager and Board Secretary

Version/change control

Version	Name	Date	Comment
v.1.0	Finance & Corporate Governance Unit	February 2020	Approved
v.2.0	Finance & Corporate Governance Unit	April 2021	Approved 30.4.21

Table of Contents

1. Introduction

1.1 This policy is produced in accordance with the NHS Counter Fraud Authority's (NHSCFA) obligations under the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act (DPA) 2018. It should be read alongside the NHSCFA's GDPR - Data Protection and its website's Privacy Policy.

1.2 This is the 'appropriate policy document' for NHSCFA that sets out how we will protect special category and criminal convictions data.

1.3 Article 9(1) of the GDPR prohibits the processing of special categories of personal information unless a condition in Article 9(2) is met, such as for a reason of substantial public interest (see Part 2, Schedule 1 of the DPA 2018). For the NHSCFA, the processing of special categories of personal data ("sensitive processing") is permitted where it is necessary for a function conferred by an enactment or a government department[1], preventing and detecting unlawful acts[2], protecting the public from dishonesty etc[3] and it is necessary for reasons of substantial public interest.

1.4 **It is important to note that NHSCFA is not an 'anti-fraud organisation' within the meaning of s.68 of the Serious Crime Act 2007 and therefore we cannot rely on the specific function of 'preventing fraud' in Part 2, Schedule 1 of the DPA 2018**.

1.5 There is a further requirement that this condition will only be met if the sensitive processing is carried out in accordance with this policy[4]. All staff must therefore have regard to this policy when carrying out sensitive processing on behalf of the NHSCFA, when acting in its capacity as 'controller' of the personal data.

1.6 Personal data about criminal offences and convictions are dealt with separately in Article 10 of GDPR. The DPA provides that the processing of such data only meets the requirements of Article 10 if it conforms to a condition set out in Part 1, 2 or 3 of Schedule 1. This requires that the controller must have an appropriate policy in place when the processing is carried out. The NHSCFA must have regard to this policy.

2. Purpose

2.1 The purpose of this policy is to explain:

[1] Para. 6
[2] Para. 10
[3] Para. 11
[4] Para. 5

- NHSCFA policies which are in place to secure compliance with GDPR data protection principles, when relying on substantial public interest conditions in Part 2 of Schedule 1 of the DPA; and
- The organisation's data handling and retention policy.

3. Scope

3.1 This policy applies to the Board and NHS staff who process, access, use or manage sensitive personal data during their course of employment.

4. What is 'special category' data?

4.1 Special category data as defined in Article 9 of GDPR, is personal data revealing any of the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

5. What are reasons of 'substantial public interest'?

5.1 The term 'substantial public interest' is not defined in the DPA or the GDPR. Some of the conditions assume that processing under that condition is always in the substantial public interest such as the 'prevention, detection and investigation of fraud[5]'.

[5] Not to be confused with the fraud prevention 'function' of an anti-fraud organisation referred to above.

5.2 Substantial public interest means the public interest needs to be real and of substance. Given the inherent risks of special category data it is not enough for an organisation to make a vague or generic public interest argument. It should be able to make specific arguments about the concrete wider benefits of the organisation's processing.

5.3 Commercial or private interests are not the same as a public interest and where the organisation needs to point to reasons of substantial public interest, it is not enough for it to point to its own interests. It is still possible for an organisation to have a private interest, it just needs to make sure that it can also point to a wider public interest.

5.4 The organisation should focus on showing that its overall purpose for processing has substantial public interest benefits. It is not necessary for it to make separate public interest arguments or show benefits each time it undertakes that processing, or for each special category data, if the overall purpose for processing special category data is for a substantial public interest.

5.5 The organisation must always be able to demonstrate that all of its processing under the relevant condition is actually necessary for that purpose and complies with the data minimisation principle.

6. Personal data relating to criminal convictions

6.1 NHSCFA also processes criminal convictions data, which also includes processing in relation to offences or related security measures. NHSCFA must identify both a general lawful basis for processing and an additional condition for processing this type of data.

6.2 The general lawful basis under Article 6(1) is:

- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The additional conditions under Article 9 (2) are:

- (f) processing is necessary for the establishment, exercise or defence of legal claims….
- (g) processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which shall be proportionate to

the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

7. Compliance with data protection principles

7.1 Lawfulness, fairness and transparency

The lawfulness of the NHSCFA's processing is derived from its official statutory functions. Transparency is provided by using a layered approach. Detailed information about how the NHSCFA uses personal data including special category data, is published in the NHSCFA's privacy policy on its website. It makes clear what data we collect, why it is required and with whom it may be shared.

Purpose limitation

The NHSCFA only processes personal data when permitted to do so by law. Personal data is collected for specific and legitimate purposes such as the prevention and detection of economic crime and other related unlawful acts against the NHS in England. Any use of NHSCFA data for a non-related NHSCFA function must have a specific lawful basis and it must be compatible with data protection obligations - the processing must therefore be proportionate and necessary.

Data minimisation

Each NHSCFA business function has a process in place to ensure that it only collects the information necessary to deliver that function. NHSCFA will not seek or where applicable, data subjects will not be asked to provide more information than is required. Additionally, NHSCFA internal guidance, training and policies require staff to use only the minimum amount of data required to enable specific tasks to be completed.

Where processing is for research and analysis purposes, wherever possible this is done using anonymised or pseudonymised data sets.

Accuracy

It is important when NHSCFA receive or provide information that it is complete, accurate and up to date. When permitted by law or when it is reasonable and proportionate to do so, NHSCFA may check this information with other organisations such as the Police, HMRC or the Home Office.

If a change is reported by a data subject to one of NHSCFA's business areas, wherever possible and appropriate this should also be used to update other

functions, both to improve accuracy and avoid the data subject having to report the same information to the one Controller multiple times.

Storage limitation

NHSCFA has a comprehensive data handling and retention policy in place which is available on Go2 and externally on the organisation's website.

Integrity and confidentiality

The NHSCFA has a range of security standards and policies based on best practice, current legal and government requirements to protect information from relevant threats. These standards are applied whether data is being processed by NHSCFA staff or a processor on its behalf.

All staff handling NHSCFA information are vetted and where required security cleared; they are also required to complete annual training on the importance of security and how to handle information appropriately.

In addition to having information governance and security policies and guidance embedded throughout NHSCFA, the organisation also has IT specialist security, cyber and resilience staff to help ensure that information is protected from risks of accidental or unlawful destruction, loss, alteration, unauthorised access or disclosure.

8. Accountability principle

8.1 NHSCFA as 'controller' shall be responsible for and be able to demonstrate compliance with the data protection principles. Our Accounting Officer is responsible for ensuring that the organisation is compliant with these principles.

8.2 NHSCFA will:

- Ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner upon request
- Carry out a Data Protection Impact Assessment for the processing of any high risk personal data and consult the Information Commissioner where the risks cannot be mitigated to an acceptable level
- Ensure a Data Protection Officer is appointed to provide independent advice on the organisation's personal data handling and that this person has access to the highest level of management within NHSCFA

- Have in place processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection legislation.

9. Retention and erasure of personal data

9.1 NHSCFA will ensure, where special category or criminal convictions data is processed, that:

- There is a record of that processing and that record will set out where possible the time limits for erasure of the different categories of data.
- Where special category or criminal convictions personal data is no longer required for the purposes for which it was collected, it will be deleted.
- Data subjects through the organisation's privacy policy, are given full information about how their data will be handled and this will include the period for which it will be stored.

10. Review

10.1 NHSCFA will formally review this document on a biennial basis.