NHS
Counter Fraud Authority

General Data Protection Regulation/ Data Protection Act 2018 Policy

April 2021

FCG-IG-CP-011
Version: 4.0

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

Document control

Document title	GDPR - Data Protection Act Policy
Intent	This is the formal policy document outlining the data protection principles. It is to be maintained by the document Author and Document Controller, in line with the F&CG Document Management Procedure.
Document reference (URN)	FCG-IG-CP-011
Version	4.0
Document status	Approved
Issue date	April 2021
Planned review date	April 2022
Author	Trevor Duplessis
Reviewed by	Ann Sturgess
Authorised by	Ann Sturgess

Version control

Version	Name	Date	Comment
v.1.0	Finance & Corporate Governance Unit	January 2018	Review May 2018
v. 2.0	Finance & Corporate Governance Unit	August 2018	Annual Review August 2019
v.3.0	Finance & Corporate Governance Unit	October 2019	Annual Review October 2020
v.4.0	Finance & Corporate Governance Unit	April 2021	Approved 30.4.21

Table of contents

1. Preamble

1.1 The General Data Protection Regulation (GDPR) 2016 came into force on 25 May 2018, together with the new Data Protection Act (DPA) 2018, replacing the previous data protection regime (DPA 1998) in the UK. The GDPR continues to apply following the UK's exit from the European Union (EU) and therefore operates in tandem with the 2018 Act.

1.2 The 2018 Act allows for the processing of sensitive and criminal conviction data in the absence of consent where justification exists, including allowing employers to fulfil obligations of employment law or to prevent unlawful acts and fraud.

1.3 Domestic UK processing of personal data for law enforcement purposes was governed by the 1998 DPA and the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014, which together established a robust regime for the protection of personal data by law enforcement.

1.4 In 2016 the EU agreed the Law Enforcement Directive (LED) to govern the processing of personal data by the police and other criminal justice agencies for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data.

1.5 To ensure a coherent regime following the country's exit from the EU, these provisions are now contained in the 2018 DPA and will apply to the domestic processing of personal data for such purposes.

1.6 Therefore references in this policy to the GDPR should also be taken to include references to the new DPA 2018. The applicable provisions of the LED are dealt with in the organisation's separate Law Enforcement Processing (Data Protection) Policy.

2. Introduction

Background

2.1 The NHS Counter Fraud Authority (NHSCFA) needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.

2.2 Personal data at NHSCFA can include employees (present, past and prospective), patients, contractors and third parties, private and confidential information as well as sensitive information, whether on paper, in electronic or other form.

2.3 Irrespective of how the information is collected, recorded and processed, person-identifiable information must be dealt with properly to ensure compliance with the GDPR and the DPA.

2.4 They require NHSCFA to comply with the seven principles relating to the processing of personal data (see Appendix A below). Under the Data Protection (Charges and Information) Regulations 2018, organisations that determine the purpose for which personal data is processed must pay the Information Commissioner's Office (ICO) a fee unless they are exempt. This new fee replaces the requirement to 'notify' or 'register', required under the old data protection regime.

2.5 Data protection legislation gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances ask us to erase it or stop using it and to seek damages where we are using it improperly.

2.6 The lawful and correct treatment of person-identifiable information by NHSCFA is paramount to the success of the organisation and to maintaining the confidence of its employees, stakeholders and service users. This policy will help NHSCFA ensure that all person-identifiable information is handled and processed lawfully and correctly.

GDPR/DPA principles

2.7 The NHSCFA has a legal obligation to comply with all relevant legislation in respect of data protection and information and IT security. The organisation also has a duty to comply with guidance issued by the Department of Health and Social Care, NHS Digital as well as other relevant guidance issued by advisory groups and professional bodies.

2.8 All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the NHSCFA. Significant penalties can be imposed upon the organisation or its employees for non-compliance.

2.9 The purpose of this policy is to outline how the NHSCFA meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the GDPR, as the key legislative and regulatory provision governing the security of person-identifiable information.

2.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B.

3. What information is covered?

3.1 Personal data within the respective legislative and regulatory provisions covers ‘any data that can be used to identify a living individual either directly or indirectly’. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

4. Policy statement

4.1 This document defines the data protection policy for the NHSCFA. It applies to all person-identifiable information obtained and processed by the organisation and its employees.

It sets out:

- the organisation’s policy for the protection of all person-identifiable information that is processed
- establishes the responsibilities (and best practice) for data protection
- references the key principles of the GDPR.

5. Principles

5.1 The objective of this policy is to ensure the protection of NHSCFA’s information in accordance with relevant legislation, namely:

- **To ensure payment of the processing fee**

  Pay annually, the relevant processing fee to the Information Commissioner’s Office in respect of the person-identifiable information the NHSCFA processes.

- **To ensure professionalism**

  All information is obtained, held and processed in a professional manner in accordance with the GDPR’s six principles.

- **To preserve security**

  All information is obtained, held, disclosed and disposed of in a secure manner.

- **To ensure awareness**

  Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

- **Data Subject's rights request**

  Prompt and informed responses to a subject's rights request.

5.2 The policy will be approved following annual review. Where review and update is necessary due to legislative changes this will be done immediately.

5.3 In accordance with the NHSCFA's equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, background or any other personal characteristic.

6. Scope of this policy

6.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need-to-know basis.

6.2 The procedure covers all person-identifiable information whether clinical or non-clinical, electronic or paper which may relate to individuals, employees, contractors or third parties about whom we hold information.

7. Policy

7.1 The NHSCFA obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

- staff and administrative records
- matters relating to the prevention, detection and investigation of fraud and corruption in the National Health Service and the wider heath service
- complaints and requests for information.

7.2 Such information may be kept in either computer or manual records. In processing such personal data NHSCFA will comply with the data protection principles set out in the GDPR/DPA.

8. Data protection responsibilities

Overall responsibilities

8.1 The NHSCFA Board, collectively known as the 'data controller' permit the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The Board have a legal responsibility for the payment of the processing fee and compliance with the GDPR.

8.2 The Board whilst retaining their legal responsibilities have delegated data protection compliance to the Data Protection Officer.

8.3 The Data Protection Officer's responsibilities have been allocated to the organisation's Information Governance and Risk Management Lead.

Data Protection Officer's (DPO) responsibilities

8.4 The Data Protection Officer's responsibilities include:

- ensuring that the policy is produced and kept up to date
- ensuring that the appropriate practice and procedures are adopted and followed by the NHSCFA
- provide advice and support to the Board on data protection issues within the organisation
- work collaboratively with Organisational Development and Governance and Assurance to help set the standard of data protection training for staff
- ensure the processing of personal information is reviewed and advise the organisation on the appropriate processing fee to be paid to the ICO
- ensure compliance with individual rights requests
- act as a central point of contact on data protection issues within the organisation.
- implement an effective framework for the management of data protection.

Line managers' responsibilities

8.5 All line managers across the organisation's business units are directly responsible for:

- ensuring their staff are made aware of this policy and any notices.
- ensuring their staff are aware of their data protection responsibilities.
- ensuring their staff receive suitable data protection training.

General responsibilities

8.6 All NHSCFA staff, including temporary and contractors are subject to compliance with this policy. Under GDPR, individuals as 'processors' working on the 'controller's' behalf can be held personally liable for data protection breaches, especially where they have received the requisite training.

8.7 All NHSCFA staff have a responsibility to inform their business unit Leads and the DPO of any new use of personal data, as soon as reasonably practicable after it has been identified.

8.8 All NHSCFA staff will, upon receiving a rights request from an individual for information or concerns about the processing of personal information, should immediately forward the request to the Information Governance Team at DPArequest@nhscfa.gov.uk.

8.9 Staff must follow the organisation's rights request procedure (see Appendix C below).

9. Monitoring

9.1 Compliance with this policy will be monitored by the Finance and Corporate Governance Unit and may be subject to periodic internal or external audit review where necessary.

9.2 The Information Governance and Risk Management Lead is responsible for the monitoring and updating of this policy document.

10. Validity of this policy

10.1 This policy will be reviewed at least on an annual basis or sooner, should the need arise under the authority of the Board. Associated data protection standards will be subject to ongoing development and review.

Appendix A - GDPR: Data protection principles

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject *('lawfulness, fairness and transparency')*

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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes *('purpose limitation')*

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed *('data minimisation')*

4. accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay *('accuracy')*

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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject *('storage limitation')*

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 *('integrity and confidentiality')*

7. the organisation must be responsible for the data it holds, demonstrating compliance with the other principles *('accountability')*

Appendix B - Summary of relevant legislation and guidance

Human Rights Act 1998

This Act binds public authorities including Health Authorities, Trusts and Primary Care Groups to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that "everyone has the right to respect for his private and family life, his home and his correspondence". However, this article also states "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act gives individuals rights of access to information (excluding personal information) held by public authorities.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the "Interception of Communications Act 1985". The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only for the purposes defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person-identifiable information and responsibility for disclosure rests with the organisation holding the information.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. NHSCFA issues each employee with an individual user id and password which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of inadvertently contravening the Act.

NHSCFA will adhere to the requirements of the Computer Misuse Act 1990, by ensuring that its staff are aware of their responsibilities regarding the misuse of computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act allows employers to intercept communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.

Information Security Management: NHS Code of Practice

The guidelines provide a framework for consistent and effective information security management that is both risk and standards-based and is fully integrated with other key NHS Information Governance areas. Without effective security, NHS information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties.

Confidentiality: NHS Code of Practice

Gives NHS bodies guidance concerning the required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their personal data.

The Caldicott Guardian Manual 2017

Provides guidelines relating to sharing of person-identifiable information and advocates the appointment of senior organisational members to the role, to ensure adherence to the principles.

Records Management: NHS Code of Practice

The code acts as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

Information Commissioner's Guidance - Use and Disclosure of Health Data

This guidance is concerned with the application of the Act with regards to the processing of information contained within 'health records'.

Receiving Data Subjects' Rights Request