NHS Grampian Data Protection Policy

Co-ordinator:	Reviewer:	Approver:
Head of Information Governance and Data Protection Officer	GAPF Polices Subgroup	Grampian Area Partnership Forum (GAPF)

Date approved by GAPF:	Effective Date:	Review Date:
18 February 2021	18 March 2021	February 2026

Uncontrolled When Printed

Version 2

The provisions of this policy, which was developed by a partnership group on behalf of Grampian Area Partnership Forum, apply equally to all employees of NHS Grampian except where specific exclusions have been identified

NHS Grampian

Data Protection Policy

This policy is also available in large print and other formats and languages, upon request. Please call NHS Grampian Corporate Communications on (01224) 551116 or (01224) 552245.

This policy has undergone Equality and Diversity Impact Assessment.

Revision History:

Document Title	Policy Version	Date approved by GAPF	Review Date
NHS Grampian Data Protection Policy	v.1	August 2017	
	v.2	18 February 2021	February 2026

NHS Grampian

Data Protection Policy

Contents

NHS Grampian

Data Protection Policy

1. Introduction

1.1 This policy represents NHS Grampian's commitment to the appropriate processing of personal data and its respect for the rights of individuals in respect of their personal information.

1.2 NHS Grampian acknowledges its responsibilities concerning the processing of personal data and will endeavour to ensure that its activities are conducted in compliance with data protection legislation.

2. Scope and definitions

2.1 The policy concerns the processing of all personal data by NHS Grampian in respect of all activity and regardless of format/media.

2.2 'Data protection legislation' is the legislation applicable in the UK concerning the requirements for the processing of personal data. Broadly, this is defined as the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018.

2.3 'Personal data' and 'special categories of personal data' are defined per Article 4 and Article 9 of the General Data Protection Regulation.

2.4 Personal data may be generally understood to be data from which any living individual can be identified either directly from the use of identifiers or specific circumstances, or as a result of indirect identification through the combination of data points and/or circumstances in aggregation.

2.5 Notwithstanding 2.4 above, it is noted that the duty of medical confidentiality extends beyond death.

2.6 Special categories of personal data are those personal data concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs; trade union membership;
- genetic data or biometric data processed for the purpose of uniquely identifying a person;
- data concerning health; or
- data concerning a person's sex life or sexual orientation.

2.7 'Processing' is any activity concerning personal data as defined by Article 4 of the General Data Protection Regulation.

2.8 Processing may generally be understood as the: creation; receipt; storage; maintenance; use; alteration; transmission; disclosure; dissemination; combination; restriction; disposal; erasure; and/or destruction of personal data.

3. Roles and responsibilities

3.1 The Medical Director, Caldicott Guardian and Senior Information Risk Owner is the responsible officer for data protection compliance.

3.2 The Data Protection Officer has those responsibilities required by the General Data Protection Regulation.

3.3 The Information Governance Team provide guidance and operational support on data protection matters, including the mitigation of data incidents.

3.4 NHS National Services Scotland Central Legal Office provide support advice as required.

3.5 System Leadership Team are the responsible Information Asset Owners for the activities aligned to them. They are required to ensure that the processing of personal data further to those activities or in respect of any projects or initiatives they

lead on behalf of NHS Grampian is conducted appropriately and in compliance with data protection legislation. They are required to seek the involvement of the Data Protection Officer per Article 38 of the General Data Protection Regulation. They are required to have due regard to the rights of individuals in respect of the processing of personal data.

3.6 All NHS Grampian staff, the staff/students of authorised partners and the staff of data processors are required to ensure that:

- any and all processing of personal data is compliant with data protection legislation;
- they adhere to the professional and contractual confidentiality requirements at all times;
- their mandatory information governance and information security training is current;
- they only access that personal data which they are authorised to do so and seek prior approval for any exceptional access;
- all data incidents are reported via the appropriate system (currently Datix) immediately upon discovery; and
- that they escalate concerns and issues regarding the processing of personal data to their managers and Information Governance for attention.

4. Lawful processing

4.1 The General Data Protection Regulation requires that NHS Grampian details why it asserts that its processing of personal data and special categories of personal data is lawful. This will be done via the provision of privacy notices provided directly to individuals in connection with any matter or uploaded to the NHS Grampian website. These will be issued as required.

4.2 Processing may only be considered lawful where one or more of the lawful bases has been identified per Article 6 (personal data) and/or Article 9 (special

categories of personal data) of the General Data Protection Regulation. In general, the principal lawful bases for the processing of personal data by NHS Grampian are:

	Patients	**Staff**
Personal data	• 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; • processing is necessary in order to protect the vital interests of the data subject or of another natural person; • processing is necessary for compliance with a legal obligation to which the controller is subject;	• processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; • processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; • 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.
Special categories of personal data	• processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of	• processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social

	health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*; • processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; • processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to	security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; • processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; • processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; • processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and

	safeguard the rights and freedoms of the data subject, in particular professional secrecy; • processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; • processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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 the interests of the data subject.	services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3***** [see note below]; • processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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 the interests of the data subject.

***** Normally per Schedule 1, Part 1 of the Data Protection Act 2018.

4.4 Where NHS Grampian wishes to claim that the processing of special categories of personal data is necessary for reasons of substantial public interest, it will do so per the requirements of Schedule 1, Part 2 of the Data Protection Act 2018.

4.5 The information concerning lawful bases for processing provided in this policy should not be considered exhaustive. NHS Grampian will select lawful bases appropriate to its activities. Individuals should refer to applicable privacy notices for additional detail.

5. Data Protection Officer

5.1 NHS Grampian is required to designate a Data Protection Officer who has the authority and responsibilities required by Articles 37, 38 and 39 of the General Data Protection Regulation. Contact details for the Data Protection Officer are provided to the Information Commissioner's Office and are published online at https://ico.org.uk/ESDWebPages/Entry/Z8547986.

6. Data controller

6.1 NHS Grampian will normally be the data controller for personal data processed further to its activities. It may also act as a joint data controller or data processor on behalf of another controller where appropriate.

7. Individual rights

7.1 NHS Grampian respects the rights of individuals in respect of their personal data. Anyone wishing to access, erase or limit the use of their information should contact the Information Governance Team in the first instance at nhsg.infogovernance@nhs.scot.

8. Additional Information

8.1 Anyone seeking additional information or guidance concerning data protection should contact the Information Governance Team in the first instance nhsg.infogovernance@nhs.scot.