NHS Borders

Data Protection Policy

Document Control	
File Name:	2021 08 25 NHS Borders Data Protection Policy.docx
Version No:	2.1
Status:	Published
Author:	Ian Merritt
Version Date:	25 08 2021
Review Date:	24 Months or as required

Authorisation Control	
Policy Owner	Ralph Roberts – Chief Executive

Version Control

Release	Date	Author	Comments
		Dave Arkless	Review & Update of Old Policy
Draft 1.0	16th June 2005	Dave Arkless	1st Draft to Caldicott Group
Draft 1.0	28th June 2005	Dave Arkless	General Consultation (intranet)
Draft 1.0	19th September 2005	Dave Arkless	Non Clinical Risk Management Group
Draft 1.0	30th September 2005	Dave Arkless	Partnership
Operational	3rd October 2005	Dave Arkless	Signed off by Chief Executive
Operational	5th July 2006	Dave Arkless	Amended address & details, page 5
Version 1.2	26th July 2011	Ian Merritt	Minor updates to contact details and formatting
Version 1.3	21 February 2014	Ian Merritt	Minor updates to contact details and formatting
Version 1.4	10 May 2016	Ian Merritt	Minor update to include reference to the Information Governance Code of Conduct
Version 2.0	22 April 2019	Ian Merritt	Rewritten for GDPR 2016 & DPA 2018
Version 2.1	25 August 2021	Ian Merritt	Minor update to refer to UK GDPR following Brexit. Inclusion of DPO role in Section 4 – Duties

CONTENTS

1. Introduction

NHS Borders acknowledges that information is a valuable asset and needs to be appropriately governed in order to support the delivery of patient care.

It is therefore of paramount importance to ensure that information is efficiently managed and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Purpose, including legal or regulatory background

This Data Protection Policy will detail how the Board meets its obligations in respect of the key legislation concerning the management of personal information, namely the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

This policy applies to all staff working for, or on behalf of, NHS Borders.

2.1. UK General Data Protection Regulation

The GDPR covers the way organisations process personal data of living and identifiable individuals. It applies to both manual records and electronic records. The term processing covers obtaining, altering, using, retention, storage, archiving and the destruction of data.

Within the GDPR there are six Data Protection Principles.

Personal information must be:-

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specific, relevant and legitimate purposes;
3. Adequate, relevant and limited to what is necessary;
4. Accurate and where necessary kept up to date;
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed;
6. Processed in a manner that ensures appropriate security of the personal data;

There is a further requirement that the Board, as controller of the personal information, shall be able to demonstrate compliance with these six principles.

2.2. Caldicott Report 1997 (revised 2013)

The original Caldicott Review of Patient Identifiable Information found that compliance with a range of information confidentiality and security requirements across the NHS was inconsistent. As a result, a list of seven recommendations, known as the Caldicott Principles, has been developed for the management of patient identifiable data:

1. Justify the purpose(s).
2. Use and transfer patient identifiable information only when absolutely necessary.
3. Only use the minimum necessary patient identifiable information.
4. Access to patient identifiable information to be on a strict need to know basis.
5. Everyone to be aware of their responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

One of the recommendations was to appoint a senior person to act as Caldicott Guardian, responsible for approving uses of patient identifiable information. As an organisation, NHS Borders is committed to adhering to the principles and implementing the recommendations of this report. NHS Borders' Caldicott Guardian is the Joint Director of Public Health.

2.3. Common Law Duty of Confidence

The "duty of confidence" is long established within common law and as such applies equally to everyone. This means that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without a lawful reason, which may include obtaining the consent of the data subject. Examples of exceptions to the common law duty, whereby information may be disclosed without the consent of the individual are:

- Where there is an overriding public interest in the disclosure, which is usually only satisfied when there is a significant risk to the safety of one or more people;
- Where disclosure of information is required by law, for example to notify a birth.

2.4. Other Relevant Legislation

Some information is restricted by law from disclosure under other Acts of Parliament and NHS standards. These include:-

- Freedom of Information (Scotland) Act 2002
- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Human Rights Act 1998
- Computer Misuse Act 1990
- Human Fertilisation and Embryology Act 1990
- Human Fertilisation and Embryology (Disclosure of Information Act) 1992

2.5. Professional Obligations

As well as an obligation to the Board, many staff members are also bound by the Codes of Conduct of their respective professional bodies and should refer to their respective organisations for details of their guidelines.

3. Definitions

Information Governance

Information Governance is a framework bringing together all the requirements, limits and best practice that applies to the handling of person identifiable data.

Personal Data

Personal data is information that relates to an identified or identifiable individual.

Special Category Data

Special category data is personal data that is more sensitive, and so needs more protection. It includes information that identifies racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, genetics, biometrics (where used for ID purposes), physical or mental health condition, sex life or sexual orientation.

Controller
The legal body, in this case NHS Borders, which determines the purpose and means of processing personal data.

Processor
Any person or organisation (other than an employee of the controller) that processes personal data on behalf of the controller.

Data Processing
Data that is processed means collecting, using, disclosing, retaining or disposing of personal data.

Data Subject
An individual who is the subject of personal data.

4. Duties

The Board has a legal duty to comply with the GDPR and the DPA.

NHS Borders Executive Team
It is the role of the Executive Team to define the policy in respect of data protection, taking into account legal and NHS requirements. The Executive Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Senior Information Risk Owner (SIRO)
The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk, acting as advocate for information risk on the Executive Team. The SIRO is also the Director responsible for the Information Governance framework. This role is undertaken by the Director of Planning and Performance.

The SIRO will delegate the day to day management of Information Governance to the Head of Information Management and Technology.

Data Protection Officer
The UK GDPR makes it a legal requirement for NHS Boards to designate a suitably qualified and resourced individual as a Data Protection Officer. The function is to provide advice to the organisation in relation to data protection law and to monitor compliance with the legislation. The DPO will be the main point of contact with the Information Commissioner's Office, the UK regulator of the Data Protection Act and GDPR. NHS Borders' DPO is the Cyber and Information Governance Manager.

Caldicott Guardian
The primary responsibility for the role of Caldicott Guardian is to safeguard and govern the uses made of patient information within the Board and the transfer of patient identifiable information outside the Board. In NHS Borders the Caldicott Guardian is the Joint Director for Public Health.

Information Governance Team
The Information Governance Team is responsible for the implementation, development and monitoring of the Information Governance framework.

All Managers
Managers within the Board are responsible for ensuring that the policy and its supporting standards are built into local processes and that there is ongoing compliance.

All Staff

All staff, whether fixed-term or permanent, on a staff Bank or external contractors, are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

Information Governance Committee Structure

The Executive Team has designated authority to the Information Governance Committee, chaired by the Medical Director, to monitor the implementation and oversee the compliance of Information Governance within NHS Borders.

The Information Governance Committee provides assurance to the Executive Team, via the Clinical Executive Operational Group.

5. Overview of the GDPR Principles

Principle 1 – Personal information must be processed lawfully, fairly and in a transparent manner

The organisation must have legitimate reasons for collecting and using personal information.

Service users and employees of NHS Borders must be aware why personal information is collected about them, how this is used and to whom it may be disclosed. The organisation will be open, honest and clear when managing personal information.

Patients will be made aware of this by means of the Privacy Notice published on the public website and information leaflets describing how their personal information is managed. In addition, other communication methods such as posters and information screens in waiting areas will be utilised as appropriate. Healthcare professionals may play an integral part in ensuring patients understand how their information will be used.

During the recruitment process and via ongoing line management, NHS Borders employees (whether permanent or temporary) should be made aware of the reasons why their information is required and how it will be used.

5.1. Fair Processing

Personal information should be treated as being obtained fairly if it is provided by a person who is legally authorised, or required, to provide it.

5.2. Lawful Processing

In order to comply with the "lawful" aspect of the first principle, a lawful basis must apply. There are five that are typically available to the NHS:

a. **Consent** – There is clear consent from the data subject to process the data
b. **Contract** – Processing is necessary to fulfil a contract with the individual
c. **Legal Obligation** – Processing is necessary in order to comply with the law
d. **Vital interests** – Processing is necessary to protect someone's life
e. **Public task** – Processing is necessary to carry out a task that is in the public interest or is an official function of a public authority

If it is not possible to apply one of the above lawful bases then the processing of personal information must not take place as it would be unlawful.

If special category data is to be processed it is necessary to identify both a lawful basis (as above) for general processing and an additional condition for processing this type of data.

There are ten available conditions but the ones most relevant to the NHS are:

- Consent
- Employment purposes
- Vital Interests
- Legal defence
- Provision of Health Care
- Public Health
- Research/Statistical

5.3. Transparent Processing

NHS Borders will only process personal information for purposes that would be reasonably expected by data subjects. The organisation's privacy notice, which details these purposes, is published here - http://www.nhsborders.scot.nhs.uk/privacy-notice/.

Principle 2 – Personal information must be collected for specific, relevant and legitimate purposes

At the outset, the NHS Borders should be transparent about why personal information is collected and how the information is used is in line with the reasonable expectations of the individuals concerned.

When service users and employees of the organisation supply their personal information for a specified purpose, then that personal data must not be used or disclosed for any other purpose that is incompatible with the original purpose(s).

An additional lawful basis would need to be identified to use or disclose personal data for a purpose that is additional to, or different from, the purpose for which it was originally obtained.

Information should only be shared if it is appropriate and necessary to do so.

Principle 3 – Personal information must be adequate, relevant and limited to what is necessary

NHS Borders should only hold sufficient personal information on service users and employees for the purpose in relation to that individual and ensure that no information is held that is not needed for that purpose.

As the organisation processes sensitive personal information, it is particularly important to ensure that only the minimum necessary is collected or retained to carry out the task.

Principle 4 – Accurate and where necessary kept up to date

The organisation must take reasonable steps to ensure the accuracy of personal information.

All staff are responsible for ensuring that personal information they process is accurate and up to date by carrying out their own quality assurance checks.

Principle 5 – Personal information must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed

The organisation must take reasonable steps to comply with this principle. The NHS Borders Records Management Policy has been developed to provide staff with detailed information on how to manage personal information relating to staff.

NHS Borders is committed to the use of the Records Management: Health and Social Care Code of Practice (Scotland) which documents the minimum retention periods for service user information.

All staff are responsible for any records that they create or use in the course of their duties, in line with the Public Records (Scotland) Act (2011), and must be aware that any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations.

Principle 6 – Personal information must be processed in a manner that ensures appropriate security of the personal data

NHS Borders recognises that it must employ suitable security measures to protect the sensitive personal data that it processes.

The Information Security Policy details the following:

- Design and description of the security measures in place for paper and electronic personal information.
- Key roles and responsibilities in respect of information security
- Details of physical and network security measures
- Details of information security training and signposting key NHS Scotland and Information Commissioner's Office policy and guidance
- How NHS Borders will deal with a breach of information security

Removable storage devices including laptops, memory sticks and DVDs/CDs must be encrypted to AES 256bit standards in line with the NHS Scotland Information Security Policy.

6. Data Subject Rights

As a Controller, NHS Borders has an obligation to ensure that the rights of individuals are appropriately respected in relation to the GDPR.

The rights it refers to are:

- Right to be informed
- Right of access
- Right to rectification
- Right to object
- Right to restrict processing
- Right to data portability
- Right to erasure
- Rights in relation to automated decision-making and profiling

Not all of the Rights are unconditional and some may not apply at all in all instances. In most cases, the lawful basis under which the processing is taking place will determine whether a data subject can invoke a particular Right. The onus will always be on organisation to justify why a Right does not apply.

6.1. Managing the Right of Access

Individuals whose information is held by NHS Borders have rights of access to it (subject to certain exemptions) regardless of the media the information may be held.

The Subject Access (medico-legal) team within the Medical Records department manages the disclosure of personal information in respect of the following:

- UK GDPR
- DPA 2018
- Access to Health Records Act 1990

All requests for access to health information received by the organisation must be directed to the Subject Access team.

Requests from members of staff for access to information held in the employment record must be directed to the Human Resources department.

7. Data Protection Impact Assessments (DPIA)

It is a legal requirement to perform a Data Protection Impact Assessment (DPIA) on any policy, process, project, system or initiative (collectively referred to as a project here) that includes the processing of personal data, before the processing commences – i.e. at the very beginning of the project. The Information Governance team and the Data Protection Officer must be consulted throughout the project and will monitor progress. The DPIA will identify any risks to personal information resulting from the intended processing and will determine the measures to address them. The DPIA template and further guidance can be found on the Policies and Procedures page of the Information Governance microsite.

8. Transferring personal information abroad

NHS Borders must take reasonable steps to ensure that personal information is not transferred abroad without suitable safeguards.

If it is necessary to send personal information, either electronically or in paper format to countries outside either the United Kingdom or the European Economic Area (EEA), it must be discussed with a senior manager. The Information Governance team and Caldicott Guardian will also be able to offer help and advice.

It is vital to ensure that any transfer of personal information is carried out securely and normally with full patient consent or for the purposes of ongoing patient care.

All person identifiable information identified that is processed outside of the UK will be subject to an individual risk assessment carried out by the Information Governance team.

9. Keeping data subjects informed

NHS Borders is required to inform data subjects about how their personal information will be managed.

There is a comprehensive privacy notice that details management of personal information on the public NHS Borders website. Other forms of media, such as information screens in waiting areas and leaflets will also be used to inform patients. Where appropriate, services may be required to produce privacy notices specific to the service they provide. The Information Governance team will provide a template and guidance as required.

Improving communication with the public will be continually monitored as part of the Information Governance responsibilities.

10. Data Protection Training

Information Governance training is made available to all staff in the organisation's mandatory and statutory online training platform, LearnPro.

The Information Governance team will also provide on-going awareness of Data Protection matters via the organisation's standard communication channels, such as the Intranet and Staff Share emails.

Key staff groups will be identified for further bespoke Data Protection training.

11. Managing Data Protection Breaches

Staff must guard against breaches of the data protection legislation by protecting information from improper disclosure at all times.

All data protection breaches must be reported on Datix, the organisation's Adverse Event Reporting System. Staff should also notify the Information Governance team of any breaches, where appropriate.

Incidents will be managed in line with the Information Governance Incident Management Procedure. NHS Borders is legally required to report to the Information Commissioner's Office (ICO) any data breaches that may result in a risk to an individual. This must be done within 72 hours of becoming aware of the incident so it is important the Information Governance team is notified as soon as possible.

Staff members who breach the GDPR or the DPA may be subject to disciplinary action in line with the HR Management of Employee Conduct Policy.

Serious breaches of Data Protection legislation will be reported to Police Scotland for consideration of prosecution

12. Role of the Information Commissioner's Office

The Information Commissioner's Office (ICO) is the UK's independent public body set up to promote access to official information and protect personal information.

NHS Borders has an obligation as a Controller to register with the Information Commissioner. This information is publically available by accessing the ICO website.

NHS Borders' Data Protection Registration number is Z772810X

13. Overall Responsibility for the Document

The Information Governance Committee is responsible for authorising this document. The Information Governance team has responsibility for the dissemination, implementation and review of this document.

14. Consultation and Ratification

The Caldicott Guardian and Information Governance Committee have approved this policy and it has been ratified by the Clinical Executive Operational Group.

15. Dissemination and Implementation

Publication of this policy has been publicised on the staff Intranet and in a Staff Share news briefing. All Departmental Heads have had the policy sent to them and the policy is available on the Information Governance microsite (http://intranet/resource.asp?uid=306).

16. Monitoring Compliance and Effectiveness

The Information Governance Committee is tasked with the responsibility of monitoring compliance of this policy.

The committee will receive quarterly update reports from the Information Governance team on all data protection breaches that have occurred. The committee will also receive statistical updates on Subject Access Requests.

Serious breaches and investigation reports will be discussed in full at the Information Governance Committee meetings with any follow up actions identified and assigned appropriately.

Compliance with this policy will also be monitored by the completion of the Information Governance online training. Compliance reports are included in the Information Governance Annual Report which is produced by the Information Governance team and submitted to the Audit Committee.

16.1. Diversity

There is no adverse impact on any group in terms of Age, Disability, Gender reassignment, Marriage and civil partnership, Pregnancy and maternity, Race, Religion and belief, Sex or Sexual orientation in relation to this procedure. The application of this policy/procedure will be monitored to ensure compliance with the organisation's Equality and Diversity Strategy.

17. References and Associated Further Reading

Document name	Web address
General Data Protection Regulation	https://gdpr-info.eu/
Data Protection Act (2018)	http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
Information Commissioner's Office	https://ico.org.uk/
Access to Health Records Act 1990	http://www.legislation.gov.uk/ukpga/1990/23/contents
General Medical Council – Confidentiality: Guidance for Doctors:	https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality
Nursing and Midwifery Council – Confidentiality	https://www.nmc.org.uk/standards/code/ https://www.rcn.org.uk/get-help/rcn-advice/confidentiality
Health and Care Professions Council – Information for Registrants: Confidentiality	http://www.hpc-uk.org/assets/documents/100023F1GuidanceonconfidentialityFINAL.pdf
Freedom of Information (Scotland) Act (2002)	http://www.legislation.gov.uk/asp/2002/13/contents
Scottish Government Records Management: Health and Social Care Code of Practice (Scotland) 2020	https://www.informationgovernance.scot.nhs.uk/wp-content/uploads/2020/06/SG-HSC-Scotland-Records-Management-Code-of-Practice-2020-v20200602.pdf
NHS Scotland Code of Practice for Protecting Patient Confidentiality	http://intranet/resource.asp?uid=16405
Human Rights Act Article 8	http://www.legislation.gov.uk/ukpga/1998/42/contents
Caldicott Report (2013)	https://www.gov.uk/government/publications/the-information-governance-review
Access to Medical Reports Act 1988	http://www.legislation.gov.uk/ukpga/1988/28/contents
Computer Misuse Act 1990	http://www.legislation.gov.uk/ukpga/1990/18/contents