BOARD PUBLIC

Confidentiality & Data Protection Policy

Printed copies must not be considered the definitive version

DOCUMENT CONTROL		**POLICY NO**.	IG - 102
Policy Group:	Information Assurance and Security		
Lead Author:	Head of Information Governance		
Lead Executive:	Medical Director/SIRO		
Scope: (Applicability)	Board wide	**Version no.**	4.1
Status:	Approved	**Implementation date:**	August 2013
Last review date:	April 2019	**Next review date**	November 2025
Approved by:	Board Management Team	**Approval date:**	30/11/2022
Equality Impact Assessed:	Yes	**Equality Impact Assessment date:**	14/10/2022
Data Protection Impact Assessed:	Not required	**Data Protection Impact Assessment Date:**	Not applicable

Policy on a page

Summary & Aim	Key Requirements
To ensure NHS Dumfries & Galloway meets its legal obligations as a data controller in maintaining the confidentiality of the personal information it processes for its staff and patients. Current relevant legislation, which forms the basis of this policy, are DPA18 and UKGDPR	• Awareness of, and adherence to, the 6 data protection principles and the Caldicott principles for all personal data processing • Demonstrating accountability, as a data controller, for all personal data processing • Promoting transparency within NHS Dumfries & Galloway in how staff and patient information is captured, processed, retained, shared, archived and destroyed
Target Audience	**Previous Names**
• All employees, bank workers, agency staff, contractors, students, volunteers etc	• Data Protection Policy

Equality and Diversity Statement
NHS Dumfries and Galloway recognise that some communities within society are more likely than others to experience discrimination, prejudice and inequalities. The Equality Act 2010 specifically recognises the protected characteristics of age, disability, sex, race, religion and belief, sexual orientation, gender reassignment, pregnancy and maternity, and marriage and civil partnership. The Fairer Scotland Duty, also requires NHS Dumfries and Galloway to actively consider how socio-economic disadvantage can be reduced when making strategic decisions. NHS Dumfries and Galloway is committed to: • promoting and advancing equality; • removing and reducing discrimination and harassment; and • fostering good relations between people that hold a protected characteristic and those who do not. This applies both in the provision of services and as our role as a major employer. NHS Dumfries and Galloway believe that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discrimination practice

CONTENTS

APPENDICES

1. PURPOSE AND RATIONALE

1.1 Confidentiality is a fundamental principle in the delivery of health care services. The personal information collected and processed by NHS Dumfries & Galloway relates to staff and patient. This data must be treated with respect to secure its integrity, protect it from inappropriate disclosure and ensure it is readily available to authorised staff when required.

1.2 NHS Dumfries & Galloway will maintain the confidentiality of the information it holds by adherence to legislated requirements, professional codes of practice and NHS Dumfries & Galloway policies and procedures.

2. POLICY AIMS

2.1 This policy explains how NHS Dumfries & Galloway meets its legal obligations and NHS standards relating to the confidentiality and security of information. The requirements outlined in this policy will be supplemented by other documentation which will provide detailed information on specific subject areas.

2.2 The requirements outlined in this policy are primarily based on the General Data Protection Regulation (2016/679 EU) which is the governing legislation for collecting and processing personal data in the EU. Following the end of the Brexit transition period on 31 December 2020, most of the EU GDPR was retained in UK law by the European Union (Withdrawal) Act 2018. The retained GDPR is known as the "UK GDPR". The UK GDPR is supplemented by the Data Protection Act 2018. However, other relevant legislation and guidance may be referenced, including other data protection laws.

2.3 NHS Dumfries & Galloway endorse the six GDPR principles and all staff who process personal information must ensure these principles are followed. In summary the principles stipulate that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Only processed for specified, explicit and legitimate purposes
- Adequate, relevant and limited for the purpose
- Accurate and up to date
- Kept in a way which permit identification and only for as long as necessary; and
- Processed in a way which ensures it is kept secure

The GDPR also promotes the principle of accountability and governance. NHS Dumfries & Galloway will ensure that all staff have the knowledge and tools required to meet its legal obligations including appropriate Data Protection training, staff communications and relevant policies and procedures.

NHS Dumfries & Galloway is also committed to adhering to the Caldicott principles when handling patient identifiable data. These principles are:

- Justify the purpose(s)
- Use personal data only when absolutely necessary
- Use only the minimum amount of personal data necessary to satisfy your purpose
- Access to personal data should be on a strict need-to know basis
- Everyone who has access to personal data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality
- Inform patients and service users how their personal information is used

3. POLICY SCOPE

3.1 This policy applies to all staff employed by NHS Dumfries & Galloway. It is also applicable to all contractors, partnership organisations, students and visitors not directly employed by NHS Dumfries & Galloway but engaged to work with, or have access to, information for which NHS Dumfries & Galloway is the data controller.

4. DEFINITIONS

4.1 Data Protection Act 2018 (DPA18) controls how personal information is used by organisations, businesses or the government. It came into effect 25th May 2018 and replaced the Data Protection Act 1998.

4.2 UK General Data Protection Regulation (GDPR) is a regulation in domestic law on data protection and privacy for all individual citizens of the UK

4.3 Data Protection Officer (DPO) required by NHS Dumfries & Galloway, under GDPR, to ensure the organisation applies the laws protecting the personal data of its patients and staff.

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

4.5 Special category data/information is personal data that requires more protection as it is sensitive. Specifically this type of data relates to an indivdual's racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, *health data* and sexual orientation. Data relating to criminal convictions is not special category data but additional rules and safeguards exist for the processing of this information due to the associated risks.

4.6 Data Controller NHS Dumfries & Galloway, as an organisation, is a data controller as we determine what information we process and why.

4.7 Data Processor is any person(s) or organisation, other than an employee of the organisation, who processes data on behalf of the controller.

4.8 Processing refers to the collection, recording, storage, usage, analysis, combining, disclosure and deletion of data.

4.9 **Staff** refers to all employees, bank workers, agency staff, contractors, students, volunteers etc

5. DUTIES / RESPONSIBILITIES

5.1 All employees working in NHS Dumfries & Galloway are bound by a legal duty of confidence to protect and keep up to date personal information they access during the course of their work. This is both a legal and contractual responsibility and also a requirement under the common law duty of confidence.

5.2 In order to ensure that both new and current staff are aware of their responsibilities in regard to confidentiality and data protection issues NHS Dumfries & Galloway will have a comprehensive training and awareness programme in place.

5.3 Personal data, which may be held in a number of formats including paper and on electronic systems, is considered to be anything which, either directly or indirectly, identifies an individual, eg name, address, email address, CHI number, employee number etc.

5.4 With respect to personal data, all staff must ensure that:

- It is effectively protected against improper disclosure when it is received, stored, transmitted or eventually disposed of
- Access to the data is on a need-to-know basis
- Accurate and up to date information is maintained on staff and patients' records
- Disclosure is limited to that purpose for which it is required and any disclosure can be appropriately justified
- All data breaches are to be reported to your line manager, the Data Protection Officer and raised as a Datix incident. Please refer to the NHS Personal Data Breach Reporting Procedure.
- All issues concerning confidentiality are referred to the Data Protection Officer in a timely manner
- Confidential data is disposed of correctly in line with current retention policy timescales. Please refer to the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2024

5.5 Chief Executive

As the Accountable Officer for NHS Dumfries & Galloway, the Chief Executive has overall responsibility for Data Protection, which is delegated to the Caldicott Guardian and Senior Information Risk Owner (SIRO) to manage.

5.6 Medical Director

I. The Medical Director has executive responsibility for the Information Assurance and Security Planning.

II. The Medical Director has responsibility for ensuring that the Information Assurance and Security Planning is adequately and appropriately resourced to complete its function.

5.7 Senior Information Risk Owner (SIRO)

The role of the SIRO is to take ownership of the organisation's information risk policy, act as an advocate for information risk on the Board and provide written advice to the Chief Executive on the content of their annual governance statement in regard to information risk. This role in NHS Dumfries & Galloway is currently fulfilled by the Medical Director.

5.8 Caldicott Guardian

The Caldicott Guardian is responsible and accountable for compliance with the Caldicott principles. This role in NHS Dumfries & Galloway is currently fulfilled by the Medical Director.

5.9 Information Assurance Committee

NHS Dumfries & Galloway Information Assurance Committee (IAC) has the responsibility to:

- Monitor compliance with legislation
- Monitor compliance with local policies, procedures and guidance
- Review and approve all information governance procedures
- Review all information governance policies prior to approval by Business Management Team

5.10 Data Protection Officer (DPO)

The appointment of a DPO for an organisation such as NHS Dumfries & Galloway is a mandatory requirement of the GDPR.

The DPO is responsible for ensuring NHS Dumfries & Galloway and its staff are kept informed and given advice, guidance and support about how to meet the obligations of the organisation as required by data protection legislation.

The DPO is responsible for monitoring compliance with GDPR and how it relates to the personal information processed by NHS Dumfries & Galloway, including the management of internal data protection activities, providing advice on data protection impact assessments, training staff and conducting internal audits.

The DPO is the first point of contact for the Information Commissioners Officer (ICO) and for individuals (employees, patients etc) whose personal information is processed by the organisation.

This role in NHS Dumfries & Galloway is currently fulfilled by the Head of Information Governance.

5.11 Head of Information Governance

The Head of Information Governance is responsible for:

- The implementation and enforcement of all Information Governance Policies, Procedures and guidelines
- Providing assistance and guidance in the production of all required information governance documentation including Data Protection Impact Assessments (DPIA), Data Processing Agreements (DPA) and Information Sharing Agreements (ISA)
- Developing, maintaining, reviewing and enforcing procedures to ensure the confidentiality of data
- Ensuring compliance with all relevant legislation and specific NHS Scotland Information Governance guidance
- Developing IG awareness training material to ensure that all staff are aware of their data protection responsibilities
- Provide additional training and awareness sessions when any training need identified.
- Monitoring, recording, investigating and reporting actual or potential data breaches
- Presenting reports to the Information Assurance Committee meeting covering such items as:
    - Complaints and breaches reported to the Information Commissioners Office (ICO)
    - Datix incidents
    - Fairwarning reports

5.12 Directors and Managers

All NHS Dumfries & Galloway directors and managers are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is continual compliance.

5.13 All Staff

Protecting and maintaining the confidentiality of all personal information is a mandatory requirements for all NHS Dumfries & Galloway staff. All staff have a commitment to adhere to the NHS Scotland Code of Practice: Protecting Patient Confidentiality.

All staff have a confidentiality clause included in their contract of employment. Staff are required to comply with all NHS Dumfries & Galloway policies and procedures relating to confidentiality and data protection matters. Mandatory Information Governance and Information Security training modules must be completed by all staff, at induction to the organisation and every two years thereafter, for the duration of their employment with the board.

User access to clinical systems is continually monitored by our Fairwarning system and any detected, or suspected, instances of inappropriate access by staff will be investigated. This could result in formal disciplinary action being taken.

Please refer to Fairwarning - Staff Guide and Fairwarning - Manager Guide for further information.

6. PROCESS / PROCEDURES

6.1 Data Protection Impact Assessment

A Data Protection Impact Assessment is an assessment tool used to identify, assess and mitigate any actual or potential risks to confidentiality which may arise from a proposed or existing process or project involving the use of personal data. Completing a DPIA helps to identify the most effective way to comply with data protection obligations and to ensure NHS Dumfries & Galloway meets the expectations of its staff and patients with regards to protecting the confidentiality of their information.
The DPIA allows services, departments and individuals to identify and resolve problems at an early stage, reducing associated costs and reputational damage which may otherwise occur.
Failure to manage confidentiality risks can result in enforcement action by the Information Commissioner's Officer (ICO), including substantial fines. The DPIA is one specific aspect of risk management which feeds into the overall risk management processes of our organisation.
To ensure ongoing compliance with DPA18, UKGDPR and Network and Information Systems Directive (NIS), NHS Dumfries & Galloway must follow due diligence when using personal information.

6.2 Information Sharing (ISA)

NHS Dumfries & Galloway has Information Sharing Agreements in place to enable the lawful sharing of personal and special category data with other organisations and agencies. The agreements provide staff with detailed and specific guidance on the the sharing of information between the stated parties.

To ensure information is shared appropriately with other parties where an ISA **is not required or appropriate**, staff must be satisfied that there is a legal basis for the requesting party to access this information prior to releasing it. Staff must consider how much confidential information it is necessary to share before disclosure in order to provide the minimum amount of confidential information necessary for the intended purpose.

Information can be disclosed when:

- required by law or under a court order with appropriate authorisation as described in the Data Protection Act 2018
- it is necessary for the prevention and detection of serious crime with appropriate authorisation as described in the Data Protection Act 2018

- it is in the public interest, such as concerns about a child or vulnerable adult
- the individual has provide explicit written consent

The list is not exhaustive and further advice can be sought from the Information Governance Team.

6.3 Subject Access Requests

The GDPR provides data subjects with the right of access to their own personal data as processed by NHS Dumfries & Galloway. Requests are submitted to NHS Dumfries & Galloway by contacting the Data Protection Team. Subject Access Request forms are available on both nhsdg.co.uk and the intranet.

A data subject is under no obligation to complete any pre-determined request form in order to obtain a copy of their personal data and requests can be made by email, social media or by phone. Proof of ID must always be requested and validated before any personal data is released.

The GDPR allows one calendar month in which organisations must respond to a Subject Access Request. If this is not possible then the requestor must be informed.

More information about Subject Access Requests can be found in NHS Dumfries & Galloway Subject Access Request Guidance available on the intranet.

6.4 Accidental Disclosure

Staff have a legal duty of confidence to keep personal data confidential and not divulge personal information as a result of a lack of attention or awareness e.g.

- conducting conversations about a patient or a colleague in public places
- lack of diligence when sending mail or emails to ensure they are properly addressed to the intended recipient
- leaving a device logged on and unlocked when unattended
- documents being left behind in meeting rooms or not collected promptly from printers

Staff are reminded that they may be held personally liable for a breach of personal data.

Staff should also be aware that significant financial penalties can be imposed on NHS Dumfries & Galloway under data protection legislation for serious breaches of personal data.

All instances of accidental disclosure must be reported in accordance with the NHS Dumfries & Galloway Personal Data Breach Notification Procedure. More information is provided in 6.8 Data Breach Reporting.

6.5 Freedom of Information

The Freedom of Information (Scotland) Act 2002 (FOISA) provides individuals with the right to request, and be given, information from a wide range of public organisations including NHS Dumfries & Galloway.

There are restrictions on the type of information that may be released under FOISA. For more information please refer to NHS Dumfries & Galloway Freedom of Information Policy.

6.6 Counter Fraud Services

NHS Dumfries & Galloway has a signed Partnership Agreement with NSS Counter Fraud Services (CFS) which covers the roles and responsibilities of the board and CFS in relation to the use of shared personal data for fraud investigations.

NHS Dumfries & Galloway is also required by Audit Scotland to take part in the National Fraud Initiative, a data matching exercise intended to deter and detect possible cases of fraud. NHS Dumfries & Galloway is required to provide key payroll data to allow comparison to be made with data provided by other public bodies.

The processing of data by Audit Scotland (or by the Cabinet Office on behalf of Audit Scotland) in data matching exercises is carried out under Part 2A of the Public Finance and Accountability (Scotland) Act 2000. It does not require the consent of the individuals concerned, as detailed in the Data Protection Act 2018, as there is an overarching legal requirement. Data matching performed by Audit Scotland is subject to the Audit Scotland Code of Data matching Practice.

6.7 Working Offsite

Staff may be required to work from another location or from home and may need to take confidential information with them. Staff should be aware that:

- taking home/removing paper documents which contain personal information is discouraged as far as is practicable
- compliance with all NHS Dumfries & Galloway policies and procedures is still required
- confidential personal data must be stored securely when at another location or at home when not being used

- confidential personal data should never be forwarded to a staff member's private email account
- confidential personal data must never be stored on a privately owned device e.g PC, laptop, tablet, mobile phone
- mobile devices such as laptops, tablets and mobile phones should always have the screen locked when not in use
- if using a mobile device in a public space (e.g. in a café, during a train journey, etc) care must be taken at all times to prevent other people being able to view the content on the screen.

6.8 Abuse of Privilege

Staff must not knowingly browse, search or access any information relating to themselves, their family, friends, colleagues or others without a legitimate purpose. Such actions will be treated as a personal data breach as defined in the GDPR and will be dealt with in accordance with NHS Dumfries & Galloway Fairwarning Procedure and NHS Scotland Workforce Policies.

6.9 Data Breach Reporting

All breaches of personal data which are discovered by NHS Dumfries & Galloway employees, agency staff, contractors, students and volunteers must be reported immediately by raising an incident on Datix. On discovery of a personal data breach the following steps must be taken:

Step 1. The data breach must be reported on Datix without delay, recording the full details of the data breach http://datix2012web.citrix.dghealth.scot.nhs.uk/datix/live/index.php

Step 2. Your line manager and the Information Governance Team must be informed that a breach of personal data has occurred. Advice must be sought without delay from the Information Governance Team to determine whether the data subject should be advised that their personal data has been breached. This will be dependent on the nature of the breach, the information disclosed and if notifying the data subject is likely to cause serious harm to their physical or mental wellbeing. dg.dataprotection@nhs.scot

Step 3. Contact data subject to advise of data breach if appropriate. This contact should be made by the service/department responsible for the breach.

Step 4. Consider any appropriate measures which can be taken to contain the breach or prevent it from becoming more serious

The Information Governance Team will investigate the data breach and take any further action necessary as described in the NHS Dumfries & Galloway Personal Data Breach Notification Procedure.

6.10 Monitoring

The effectiveness of this policy will be monitored by the Information Assurance Committee on a quarterly basis using input from the following sources:

- data breaches reported via Datix or directly to the Information Governance Team
- Fairwarning reports
- complaints relating to personal data processed by NHS Dumfries & Galloway
- complaints to the ICO regarding NHS Dumfries & Galloway's use of personal data, breaches of confidentiality, unnecessary processing, etc.

7 CONSULTATION

7.1 Consultation on the Confidentiality and Data Protection Policy was led by the Lead Author and included:

- Information Assurance Committee
- Board Management Team
- Data Protection Officer
- Equality & Diversity Lead
- Staff side representative

8 TRAINING AND SUPPORT

8.1 All NHS Dumfries & Galloway employees, bank workers, agency staff, contractors, students, volunteers or anyone who processes information for which NHS Dumfries & Galloway is the data controller must satisfy a minimum Information Governance & Security training requirement of once every two years, as recommended by the Information Commissioner's Office.

8.2 Training and awareness sessions on confidentiality and data protection are available, on request, from the Information Governance Team.

8.3 Should anyone require further assistance or support on any of the processes or procedures set out in this policy they can contact the Information Governance Team.

9 MONITORING

9.1 The monitoring arrangements for this Policy are set out in the table below.

Element to be monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Compliance with legislation (DPA18/GDPR)	Review of Datix incidents, ICO reports, complaints	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly
Compliance with local policies, procedures, guidelines	Review of Fairwarning reports, Datix incidents, ICO reports, complaints	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly
Data Breaches (incl. inappropriate access)	Datix	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly
Compliance with mandatory IG/IS training requirement	LearnPro reports	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly
Completion of required IG/IS documentation	Review of registers: DPIAs, ISAs, DPAs, SSPs	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	

9.2

10 EQUALITY IMPACT ASSESSMENT

10.1 An Equality Impact Assessment was completed on 14/10/2022. The completion of an EIA will be considered during each subsequent review of this policy.

11 DATA PROTECTION IMPACT ASSESSMENT

11.1 A Data Protection Impact Assessment (DPIA) is not required for this policy.

12. DOCUMENT CONTROL SHEET

12.1 Document Amendment History

Version	Section(s)	Reason for update
0.1	NHS Lanarkshire exemplar document	Editing required for NHS Dumfries & Galloway purposes
1.0	ALL	1st draft
1.1	ALL	2nd draft
1.2	ALL	Final draft following review and amendments as recommended by the Information Assurance Committee – Key Points added.
1.3	ALL	Final recommendation for approval by APF
1.4	ALL	Updates for Public Records (Scotland) Act 2011
2.0	ALL	Updates for SG Information Security Framework DL2015/17
3.0	ALL	Document rewritten to incorporate changes required by GDPR/DPA18. Title changed to make it easier to find on NHSDG intranet. Reduced detailed content now available in separate subject specific documents
4.0	ALL	Transferred to new policy document template approved March 2022, reviewed in accordance and with reference to Policy Management Policy reviewed January 2022, and Document Development checklist. Includes references to approved data breach/SAR procedures.
4.1	Section 5.4	Updated Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2024

12.2 Distribution

Name	Responsibility	Version number
Corporate Business Manager	Update Policy Register	4.0
Information Assurance Committee	For comment	4.0
Board Management Team (BMT)	For approval	4.0
Information Governance Team	To place on intranet and monitor policy compliance	4.0
Communications	Place in ‘latest news’	4.0

12.3 Associated documents

NHS Dumfries & Galloway Information Security Policy
NHS Dumfries & Galloway Information Assurance Strategy
NHS Dumfries & Galloway Access to Information Systems Procedure
NHS Dumfries & Galloway Mobile Devices Policy
NHS Dumfries & Galloway Acceptable Use of Email
NHS Dumfries & Galloway Acceptable Use of the Intranet and Internet
NHS Dumfries & Galloway Personal Data Breach Notification Procedure
NHS Dumfries & Galloway Subject Access Request Procedure
NHS Dumfries & Galloway Freedom of Information Policy
Audit Scotland Code of Data Sharing Practice
NHS Scotland Counter Fraud Services – Partnership Agreement with Health Boards 2019-2022

12.4 Action Plan for Implementation

Action	**Lead Officer**	**Timeframe**
Update policy register	Corporate Business Manager	Immediate
Place in 'latest' news	Communications	Immediate
Place on intranet	Head of Information Governance	Immediate
Dissemination to all staff through line management	General Managers	Continual availability of policy document on intranet.