Confidentiality & Data Protection Policy

Printed copies should not be considered the definitive version

DOCUMENT CONTROL	**POLICY NO.**	**IG-102** (Ref: IG POL 2019 – 001)	
Policy Group	Information Assurance and Security		
Author	John McGonigle	Version No.	3.0
Reviewer	Information Governance Group	Implementation Date	Aug 2013
Scope (Applicability)	Board wide	Next review date	April 2021
Status	Final draft for approval	Last review date	April 2019
Approved By	APF Information Governance Group		
Impact Assessed:	Yes April 2019		

Contents

1. OVERVIEW

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

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

2. POLICY AIMS

This policy details 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 to provide detailed information on specific subject areas.

The requirements outlined in this policy are primarily based upon the General Data Protection Regulation, Regulation (EU) 2016/679, (GDPR) and the Data Protection Act 2018 (DPA18) however other relevant legislation and guidance may be referenced, including other data protection laws.

NHS Dumfries & Galloway endorse the six GDPR principles and all staff that 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 ('lawfulness, fairness and transparency')
- Only processed for specified, explicit and legitimate purposes ('purpose limitation')
- Adequate, relevant and limited for the purpose ('data minimisation')
- Accurate and up to date ('accuracy')
- Kept in a way that permits identification and only for as long as necessary ('storage limitation'); and
- Processed in a way that ensures it is kept secure ('integrity and confidentiality')

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 and Galloway is also committed to adhering to the Caldicott principles for handling patient- identifiable data, i.e:

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential 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

3. SCOPE & APPLICABILITY

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 who have access to health board information.

4. ROLES & RESPONSIBILITIES

All employees working in NHS Dumfries and 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.

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 and Galloway will ensure there is a comprehensive training and awareness programme in place.

Person identifiable data, which may be held in a number of formats including paper and electronic systems, can be considered as anything which contains the means, either directly or indirectly, that enables the identification of an individual to be made, e.g., name, address, email address, CHI number, employee number, etc.

With respect to person identifiable confidential 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 reported to your line manager and also raised as a Datix incident
- 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

a. Chief Executive

As the Accountable Officer for the Health Board, the Chief Executive has overall responsibility for Data Protection, which is delegated to the Caldicott Guardian and Senior Information Risk Owner to manage.

b. Medical Director

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

c. SIRO

The role of the Senior Information Risk Owner (SIRO) is to take ownership of the organisations' 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 position is currently held by NHS Dumfries and Galloway Medical Director.

d. Caldicott Guardian

The Caldicott Guardian is responsible and accountable for compliance with the Caldicott principles. This position is currently held by NHS Dumfries and Galloway Medical Director.

e. Information Assurance Committee

The 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 to approve all Information Governance policies

- report quarterly to the Audit and Risk Committee on levels of compliance with policy.

f. Data Protection Officer

The appointment of a Data Protection Officer (DPO) for an organization like NHS Dumfries and Galloway is a mandatory requirement of the GDPR.

The DPO is responsible for ensuring that NHS Dumfries and Galloway and its staff are kept informed and given advice about how to meet our obligations under all data protection legislation.

The DPO is responsible for monitoring compliance with GDPR and how it relates to the personal information processed by NHS Dumfries and Galloway, including managing 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 Office (ICO) and for individuals (employees, patients, etc) whose personal information is processed by NHS Dumfries & Galloway.

g. 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 Information Sharing Agreements (ISA) and Data Protection Impact Assessments (DPIA)
- 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
- 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

h. 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 on-going compliance.

i. All Staff

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

All staff also have a confidentiality clause included in their contract of employment. Staff are also required to comply with all NHS Dumfries & Galloway policies and procedures relating to the confidentiality and data protection matters. Relevant training will be provided to staff both at induction and on an ongoing basis to ensure they are kept updated on data protection and confidentiality issues.

5. DISCLOSURE OF INFORMATION

a) Information Sharing

NHS Dumfries & Galloway has Information Sharing Agreements in place to enable the lawful sharing of personal and other relevant information with other agencies. These provide staff with detailed and specific guidance on the sharing of information between relevant parties.

To ensure information is only shared appropriately with other parties where an Information Sharing Agreement **is not required or appropriate**, then staff must take care to ensure there is a legal basis for access to the information before releasing it. Staff must consider how much confidential information is required before disclosure and ensure that only the minimum amount of confidential information is disclosed and is appropriate for the intended purpose.

Information can be disclosed:-

- When required by law or under a court order with appropriate authorisation as set out in the Data Protection Act 2018
- Prevention and detection of serious crime with appropriate authorisation as set out in the Data Protection Act 2018
- When in the public interest, such as concerns about a child or vulnerable adult
- With the explicit written consent of the individual

This list is not exhaustive and further advice can be sought from the Information Governance Department.

b) Subject Access Requests

The GDPR provides data subjects with the right to access to personal data that NHS Dumfries & Galloway holds about them. Requests are submitted to NHS Dumfries & Galloway using the appropriate Subject Access Request form which is available on both the NHS Dumfries & Galloway internet page and on Beacon.

The GDPR now also allows requestors to submit requests by email or telephone without the need to complete a Subject Access Request form. However proof of ID must always be requested and validated before any data is released to the requestor.

GDPR stipulates that organisations must respond to a Subject Access Request within one calendar month and i this is not possible then the requestor must be informed.

c) Accidental Disclosure

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

- holding conversations that might be heard in public places about a patient or colleague
- not taking care when sending mail or emails to ensure that they are properly addressed
- documents left behind in meeting rooms or printers

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

You should also be aware that significant financial penalties can be imposed on NHS Dumfries and Galloway under Data Protection legislation for serious breaches of personal data.

d) Freedom of Information

The Freedom of Information (Scotland) Act 2002 (the FOI Act) provides individuals with the right to ask for 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 the FOI act. For more information refer to the Freedom of Information documentation available on the intranet.

e) Counter Fraud Services

We have a signed Partnership Agreement with NSS Counter Fraud Services (CFS) which amongst other things covers the roles and responsibilities of the Health Board and CFS in relation to the used of Shared Personal Data for fraud investigations.

We are 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. We are therefore required to provide key payroll data so that it can be compared with data provided by other public bodies.

The processing of data by Audit Scotland (or by the Cabinet Office on Audit Scotland's behalf) in a data matching exercise is carried out under the powers in Part 2A of the Public Finance and Accountability (Scotland) Act 2000. It does not require the consent of the individuals concerned under the Data Protection Act 2018. Data matching by Audit Scotland is subject to the Audit Scotland Code of Data Matching Practice.

6. WORKING OFFSITE

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

a) The taking home / removing paper documents containing personal data should be discouraged as far as is practical;
b) Compliance with all NHS Dumfries and Galloway policies and procedures is still required
c) Confidential data must be stored securely when at another location or at home when not being used;
d) Personal data should not be forwarded to a private email account
e) Confidential data must not be stored on a privately owned computer, device or on a non NHS Dumfries & Galloway mobile telephone.
f) Mobile devices such as laptops, tablets and mobile phones should have the screen locked when not in use.
g) When using mobile devices in public spaces (e.g. in a café, on a train journey, etc) care should be taken at all time to prevent others being able to view the content on screen.

7. ABUSE OF PRIVILEGE

Staff **must not** knowingly browse, search for or look at any information relating to themselves, their own family, friends, colleagues or others without a legitimate purpose. Such actions will be treated as a personal data breach as defined by the GDPR and may be dealt with in line with the NHS Dumfries & Galloway Disciplinary Policy and Procedure.

Audits of staff use of systems are performed by the Information Governance Department using the Fairwarning Monitoring tool and the results passed to the Workforce Department for action.

8. DATA BREACH REPORTING

All breaches of personal data discovered by NHS Dumfries and Galloway employees, agency staff, contractors, students and volunteers must be reported 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

Step 2. Your line manager must be informed that a data breach of personal data has occurred

Step 3. If the severity of the breach is thought to be serious contact the Data Protection team immediately

Step 4. If possible take appropriate action to prevent the data breach becoming more serious

The Data protection team will investigate the data breach and take any further action necessary as described in the NHS Dumfries & Galloway Data Breach Reporting Procedure.

9. 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 Data Protection team
- Fairwarning reports
- Complaints about data submitted to NHS Dumfries & Galloway
- Complaints to the ICO regarding NHS Dumfries & Galloway s' use of data, breaches of confidentiality, etc

10. EQUALITY AND DIVERSITY

NHS Dumfries and Galloway have a responsibility under the Equality Act 2010 to pay due regard to the following aims, in relation to the 9 protected characteristics of Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex and Sexual Orientation, to:

- Eliminate discrimination, harassment and victimisation
- Advance equality of opportunity between those who share a protected characteristic and those who do not by:-
    - Removing or minimising disadvantages suffered by people because of their protected characteristic

- Taking steps to meet the needs of people from protected groups where these are different from the needs of other people
- Encouraging people from protected groups to participate in public life or in other activities where their participation is proportionately low.

• Foster good relations between those who share a protected characteristic and those who do not.

Any data that is gathered on a person's protected characteristics to help the Board meet the above aims is covered by this policy.

The Board will ensure that the Confidentiality and Data Protection Policy does not discriminate against members of staff either in the way it has been designed or the how it is implemented in practice.

NHS Dumfries and Galloway will not tolerate behaviours that may constitute a lack of respect for others, discrimination, harassment or victimisation of its staff in the course of their employment. Nor will it tolerate such behaviour by its staff whether directed against colleagues or other people with whom they come into contact during the course of their employment.

11. DOCUMENT CONTROL SHEET

Document Status

Title	Confidentiality & Data Protection Policy
Author	John McGonigle
Approver	Information Assurance Committee
Document reference	
Version number	3.0

Document Amendment History

Version number	Edited by	Edit date	Topics covered
0.1	NHS Lanarkshire exemplar document	June 2009	Exemplar document
1.0	Andrew Turner	25th March 2013	1st Draft.
1.1	Graham Gault	2nd July 2013	2nd Draft
1.2	Andrew Turner	11th July 2013	Final draft following review and amendments as recommended by Information Assurance Committee – Key Points added
1.3	Andrew Turner	8th August 2013	Final recommendation for approval by APF
1.4	Andrew Turner	2nd November 2015	Updates for Public Records (Scotland) Act 2011
2.0	Andrew Turner	19th December 2016	Updates for SG Information Security Framework DL2015/17
3.0	John McGonigle	12th April 2019	• Document rewritten to incorporate changes required by the GDPR and DPA18. • Title changed to make it easier to find on the NHS D&G Intranet • Reduced detailed content which will now be available in separate subject specific documents.

Distribution

Name	Version number	Responsibility
Corporate Business Manager	3.0	Place on policy register
Information Assurance Committee	3.0	For approval
Area Partnership Forum	3.0	For approval
Staff side representative	3.0	For comment prior to presentation to APF
Data Protection Department	3.0	To monitor compliance with policy
Communications Team	3.0	Place on Intranet and in 'latest' news'

Associated Documents

NHS Dumfries & Galloway Information Security Policy
NHS Dumfries & Galloway Information Assurance Strategy
NHS Dumfries & Galloway Information Systems Procurement, Development and Implementation Procedure
NHS Dumfries & Galloway Access to Information Systems Procedure
NHS Dumfries & Galloway Mobile Devices Policy
NHS Dumfries & Galloway Guide to the Acceptable Use of eMail
NHS Dumfries & Galloway Guide to the Acceptable Use of Internet and Internet
NHS Dumfries & Galloway Data Breach Reporting 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

Communication Action Plan for Implementation

Name	Responsibility	Timeframe
Place on policy register	Corporate Business Manager	Immediate
Place in 'latest' news'	Communications Team	Immediate
Place on Intranet	Communications Team	Immediate
Dissemination to all staff through line management	Board Management Group	Continual availability of document on Intranet.

Appendix 1

The principal legislation relevant to confidentiality and data protection in NHS Dumfries and Galloway is listed below:

- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA18)
- Computer Misuse Act 1990
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Health and Social Care Act (2001)
- Freedom of Information (Scotland) Act (2002)
- Public Records (Scotland) Act (2011) (PRSA)
- Electronic Communications Act (2000)
- The Privacy and Electronic Communications Regulations (PECR)