Information Governance Policy

Document Control	
Document ID	
Document title	Information Governance Policy
Version	8
Version status / number	Draft
Date ratified	1 November 2023
Approving body	Finance and Audit Committee
Name and job title of lead author	Kathryn Wise, Information Governance Lead
Date published	January 2024
Review date	July 2024

Version Control Sheet

The table below logs the history of the steps in development of the document and detail of where changes were made and why, for example in response to feedback.

Version	Date	Author	Status	Comments
1	Nov 13	V Linford	Draft	Current document expired and requires review
2	July 15	V Linford	Draft	Revision of committees and responsibilities
3	September 15	V Linford	FINAL	Approved by Finance & Performance Committee
4	June 16	V Linford	Review	Amendments to Committee names only.
4	July 16	V Linford	Review	Approval by IG Group. To be forwarded to Finance, Performance & Business Change Committee
4	Oct 16	V Linford	Final	Approved at Finance, Performance & Business Change
5	January 17	V Linford	Draft	Minor changes made to Committee Names
5.1	February 17	V Linford	Draft	Inclusion of IG Group in accountability and removal of HSCIC training tool as a training source. Inclusion of training requirements.
5.2	February 2017	T Cooper	Draft	Amendments required following internal audit review to strengthen the policy. Inclusion of Head of Compliance Role (p4), Inclusion of additional supporting policies (p 7)
6	2/03/2017	T Cooper	Final	To be uploaded to the intranet as agreed
6.1	07/06/18	T Cooper	Draft	Reviewed to amend to show changes to group names and to add references to GDPR. Toolkit sections updated

6.2	08/05/19	T Cooper	Draft	Changes made to the standards linked to the DSP Toolkit (section 2.1) Changes to titles Associated policy list updated(section 10) Purpose added to the policy(section 2)
7	22/05/2019	T Cooper	Review	For approval at DPG 04/06/19 - DPO reviewed and no changes recommended. To be presented at FPBC on 13/06/19
7.1	06/12/22	IG Manager	Review	Policy review date extended to June 2023
7.2	July 2023	Kathryn Wise	Review	Minor corrections, amended GDPR to UK GDPR
7.3	01/11/23	Kathryn Wise	Review	Policy approved at Finance and Audit Committee on old template
7.4	23/11/23	Lois Pape Senior Administrator	Review	Policy transferred to new template
7.5	19/01/24	Sharon Hardcastle Director of Finance	Review	Updated policy approved by Lead Exec
8	19/01/23	Lois Pape	Final	Document and version control updated. Request upload to intranet.

Contents

Policy

Spectrum Community Health CIC provides quality healthcare interventions for people in vulnerable circumstances. We work in partnership to provide primary care, substance misuse and sexual health services, in the community and in secure environments including prisons, hospitals and immigration centres. As a not-for-profit social business, we are committed to addressing health inequalities and investing in the health and wellbeing of the communities we serve.

Spectrum recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources and will ensure a robust information governance framework is in place in which to manage information.

Equality Impact Assessment Summary

Assessment criteria	Outcome
What is the policy seeking to achieve?	This policy intends to provide clear guidance on Information Governance for Spectrum CIC
Who will be affected by the policy and why?	All Staff
Who has the policy been written with consideration to?	• UK General Data Protection Regulations (UK GDPR)- Data Protection Act 2018 • Freedom of Information Act • Access to health records Act 1990 • Computer Misuse Act 1990 • Human Rights Act 1998 (Including Section 23) • Confidentiality: NHS Code of Practice • Caldicott2 Principles • The common law duty of confidentiality • The Health and Social Care Act 2012 • The Information Security NHS Code of Practice

Impact Analysis

Based on available information, an assessment of the current situation and the changes being proposed, is there a possibility of a different impact (positive or negative) on the groups listed:

Group	Yes / No	Group	Yes / No
Disability	No	Gender reassignment and transgender	No
Gender / Sex	No	Religion or beliefs	No
Race	No	Pregnancy and maternity	No
Age	No	Marriage and Civil Partnerships	No
Sexual Orientation	No	Carers	No

Rationale

This policy has no impact on the above groups.

Assessment completed by

Name: Kathryn Wise

Date:

3 January 2024

Procedure

1. Introduction

Information Governance plays a key part in supporting clinical governance, service planning and performance management. Information Governance addresses the demands that law, ethics and policy place upon information processing – holding, obtaining, recording, using and sharing of information. It is crucial to ensure that staff are aware of these demands and the implications for patient care. This policy sets out how this will be achieved.

This policy is underpinned by the following legal and statutory requirements:

- UK General Data Protection Regulations (UK GDPR)-Data Protection Act 2018
- Freedom of Information Act
- Access to health records Act 1990
- Computer Misuse Act 1990
- Human Rights Act 1998 (Including Section 23)
- Confidentiality: NHS Code of Practice
- Caldicott2 Principles
- The common law duty of confidentiality
- The Health and Social Care Act 2012
- The Information Security NHS Code of Practice

Spectrum has a comprehensive range of policies (Section 10) supporting the Information Governance agenda; reference must be made to these alongside this policy. Legal and professional guidance/codes of conduct should also be considered where appropriate.

2. Scope

The purpose of this policy is to cover:

- All aspects of information within the organisation, including (but not limited to):
    - Patient/Client/Service User Information
    - Personnel/staff Information
    - Organisational Information
- All aspects of handling information, including (but not limited to):
    - Structured record systems- paper and electronic
    - Transmission of information- e-mail, post and telephone
- All information systems purchased, developed and managed by/or behalf of the organisation.

There are four key interlinked strands to the Information Governance Policy

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

This policy applies equally to all staff that work for Spectrum Community Health (including those on temporary or honorary contracts, secondments, bank staff and students). It also applies to relevant people who support and use our systems.

2.1. Guidance Notes

Spectrum will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Digital Data Security and Protection toolkit (DSPT) which defines the standards of best practice.

The DSPT is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's ten data security standards. It draws together the legal rules and central guidance and presents them as a central set of data security and protection requirements.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly. Spectrum has to assess itself against 100 mandatory requirements grouped under the following categories:

- Personal Confidential Data
- Staff Responsibilities
- Training
- Managing Data Access
- Process Reviews
- Responding to Incidents
- Continuity Planning
- Unsupported Systems
- IT Protection
- Accountable Suppliers

3. Responsibilities, accountabilities and duties

3.1. Spectrum Board

The Board is responsible for ensuring that the necessary support and resources are available for the effective implementation of this Policy.

3.2. The Data Protection Group

The Data Protection Group (DPG) is the key governing body for all Information Governance (IG) policies, including IG incidents and also has responsibility for Information Asset Owners. It has overall responsibility for the development, monitoring and review of Spectrum's IG and Data Security agenda.

3.3. The Finance and Audit Committee

The Finance, Performance and Business Change Committee are responsible for the approval of this policy.

3.4. Director of Finance

The Director of Finance is the Senior Information Risk Owner (SIRO) and has organisational responsibility for all aspects of Information Governance, including the responsibility for ensuring Spectrum has appropriate systems and policies in place to ensure that Spectrum has robust Information Governance procedures in place.

3.5. Director of Nursing and Quality Assurance/Caldicott Guardian

The "Director of Nursing" is Spectrum's Caldicott Guardian The aim of the Caldicott Guardian is to ensure patient identifiable information is shared only for justifiable purposes and that only the minimum information required is shared in each case.

Caldicott Principles:

- Justify the purpose for using confidential information
- Only use the information when absolutely necessary
- Use the minimum that is required
- Access should be on a strict need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

Caldicott Guardian Role:

1. Act as the conscience of the organisation
2. Work as part of wider IG
3. Enabler for appropriate information sharing

Advice should be sought from the Caldicott guardian when:

- Requests are received from police to access patient information
- Requests from patients to delete records
- There are actual or alleged breaches of confidentiality

3.6. Information Asset Owners

Information Asset Owners (IAO) are identified staff who are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets (systems, programmes and bodies of information) that they are responsible for.

3.7. Heads of Service

Heads of Service are responsible for ensuring that they and their staff are trained, and are familiar with the content of this policy.

3.8. Information Governance Lead

Spectrum has a dedicated Information Governance Lead who is responsible for providing specialist advice and support on all aspects of Information Governance, including reviewing this policy and ensuring it is updated in line with any changes to national guidance or local policy.

3.9. Employees

All employees are responsible for:

- Ensuring compliance with this policy
- Seeking advice, assistance and training where required

4. Procedure / implementation

4.1. Openness

- Spectrum recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Non-confidential information relating to Spectrum and its services should be available to the public through a variety of media and will continue to establish and maintain policies to ensure compliance with the Freedom Of Information Act
- Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and legislation as laid out in the UK GDPR and the Data Protection Act 2018.
- Patients will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients, staff and the public. See Subject Access Request Procedure

Spectrum will have clear procedures and arrangements for liaison with the press and broadcasting media supported by the Head of Marketing and Communications to ensure national and local guidelines are followed.

4.2. Legal compliance

- Spectrum regards all identifiable personal information relating to patients as confidential and compliance with legal and regulatory framework will be achieved, monitored and maintained.
- Spectrum regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- Spectrum will establish and maintain policies and procedures to ensure compliance with the UK General Data Protection Regulation, Data Protection Act 2018, Human Rights Act, and the common law duty of confidentiality.
- Spectrum has established and will maintain policies for the controlled and appropriate sharing of information with other agencies/partners, taking into account of relevant legislation (e.g. Crime and Disorder Act, Protection of Children Act).
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided via the ESR E-Learning Portal.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable information governance controls are in place.

4.2.1. Information Security

- Spectrum will establish and maintain policies for the effective and secure management of its information assets and resources.

- Audits will be undertaken or commissioned to assess information and IT security arrangements annually in line with NHS Digital Information Governance statement of Compliance (IGSoC)
- Spectrum Incident Reporting system will be used to report, monitor and investigate all breaches of confidentiality and security.
- Spectrum will ensure that the security of the information it holds complies with national guidelines.

4.2.2. Information Quality Assurance

- Spectrum will establish and maintain policies for information quality assurance and the effective management of records.
- Audits will be undertaken or commissioned Spectrum's quality of data and records management arrangements
- Managers will be expected to take ownership of, and seek to improve, the quality of data within their services with regular random sample audits.
- Wherever possible, information quality will be assured at the point of collection.
- Spectrum will promote data quality through policies, procedures/user manual and training

4.3. Training needs

Spectrum will provide basic Information Governance training through induction including appropriate use of Spectrum's email system. All training throughout Spectrum is recorded by the Workforce Services Department. The Data Protection Group is responsible for providing clear guidelines on the expected working practices for staff and the consequences of failing to follow policies and procedures. The Data Protection Group is also responsible for ensuring that all staff receives training which is appropriate to their role.

4.4. Implementation and dissemination

Following ratification by the Finance and Audit Committ, this policy will be available on the Intranet.

This Policy will be reviewed annually or in line with changes to relevant legislation or national guidance.

5. Training implications

Document Title	Information Governance Policy
Staff groups requiring training	All Staff
Is the training role specific	The SIRO, Caldicott Guardian, Deputy Caldicott Guardian and the IG lead have all undertaken role specific training. All staff receive IG awareness as part of Induction training and undertake annual mandatory refresher training.

Description of training	E-Learning Induction Specific training where identified from walk rounds, incidents and audits
Existing course available	E-Learning Data Security Awareness level 1
Name of training provider	NHS Digital
Frequency of training NB: Do not use the term Ad Hoc	Annual
Length of training	
Delivery method	E learning, sessions on teams or face to face
Key references / legislation	UK GDPR Data Protection Act 2018 Common Law Duty of Confidentiality Freedom of Information Act 2000
Location of training records:	ESR

6. Monitoring arrangements

An assessment of compliance with standards, within the NHS Digital's Data Security and Protection Toolkit will be undertaken at regular periods and a final submission made annually. These reports alongside a proposed work programme will be presented to the Finance and Performance Committee for information. The standards are grouped into the following initiatives:

- Personal Confidential Data
- Staff Responsibilities
- Training
- Managing Data Access
- Process Reviews
- Responding to Incidents
- Continuity Planning
- Unsupported Systems

- IT Protection

7. Links to any associated documents

Data Protection Impact Assessment Procedure (DPIA) Data Protection and Confidentiality Policy

Network Security Policy

Internet Policy Email Policy

Media Handling Policy Records Management Policy Corporate Governance Policy

Comprehensive Incident Reporting Policy Procedures (Spectrum) Data Breach Escalation Procedure

Subject Access Request Procedure and Guidance

8. References

- UK General Data Protection Regulations (UK GDPR)-Data Protection Act 2018
- Freedom of Information Act
- Access to health records Act 1990
- Computer Misuse Act 1990
- Human Rights Act 1998 (Including Section 23)
- Confidentiality: NHS Code of Practice
- Caldicott2 Principles
- The common law duty of confidentiality
- The Health and Social Care Act 2012
- The Information Security NHS Code of Practice

9. Appendices

There are no appendices within this policy.

10. Definition of Terms

The words used in this policy are used in their ordinary sense and technical terms have been avoided.