Vida Healthcare

Information Governance Policy

Version	Author	Next Review Date	Notes
V1 (March 22)	Emma Kitcher, DPO	March 23	Should be read as new policy that replaces IG01. However, largely the same but now includes Section 2 Quick Ref points Also now includes responsibilities of System Admin to oversee asset under section 6

Contents

1. INTRODUCTION

Information Governance (IG) is a set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an organisational level. Information Governance supports our immediate and future regulatory, legal, risk, environmental and operational requirements.
Information is a vital asset, both in terms of the organisational development and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

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

Vida Healthcare recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. We fully support the principles of clinical and corporate governance and recognise the power of public accountability. Equally, we place importance on the confidentiality of and the security of information about patients, the public and staff as well as commercially sensitive information. Vida Healthcare also recognises the need to share information with commissioners, partners and other third parties in a controlled manner, consistent with the established lawful basis.
This overarching Information Governance Policy and the associated protocols sets out our approach with respect to the governance of;

- Data Protection and Privacy
- Information and Cyber Security
- Data Quality and Records Management

2. QUICK REFERENCE POINTS

- Information Governance (IG) is our organisational approach to managing information
- Information is very important to the practice.
- This doesn't just mean patient data, but also information about how we run the practice.
- We have to strike a good balance between being open and transparent – because this is part of delivering a public service
- But also maintaining confidentiality so that we are trusted by those who use our services or who work with us
- The policy and the protocols beneath it help staff with Data Protection and Privacy, Information and Cyber Security, Data Quality and Records Management
- There are key roles that support this work – the SIRO, the Caldicott Guardian and the Data Protection Officer

3. KEY DEFINITIONS

Personal Confidential Information	This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

4. SCOPE

This policy applies to all practice staff whether temporary or permanent.
This overarching Information Governance Policy and the associated protocols sets out our approach with respect to the governance of;

- Data Protection and Privacy
- Information and Cyber Security
- Data Quality and Records Management

5. KEY LEGISLATION / FRAMEWORK

This policy serves to support staff to navigate and comply with the complex framework within which Information Governance operates.
This framework includes but is not limited to;

- NHS Act 2006
- Health and Social Care Act 2012
- Data Protection Act 2018 / UK General Data Protection Regulations
- Human Rights Act 1998
- Common Law Duty of Confidence
- Computer Misuse Act 1990
- Mental Health Capacity Act 2005
- Children Act 1989
- NHSX Records Management Code of Practice
- DH Information Security Code of Practice
- DH Confidentiality Code of Practice

6. ACCOUNTABLE PARTIES

The Exec / Senior Partners

The Exec / Senior Partner have overall responsibility for Information Governance at Vida Healthcare As the senior accountable officers, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to provide the necessary assurance to internal and external stakeholders.

They have particular responsibility for ensuring that Vida Healthcare meets its corporate legal responsibilities, and for the adoption of internal and external governance requirements.

Senior Information Risk Officer (SIRO)

The SIRO;

- leads and fosters a culture that values, protects and uses information for the success of the organisation and benefit of its customers.
- owns the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners / Administrators.
- Owns the organisation's information incident management framework.

System Administrators / Information Asset Owners (IAOs)

Where nominated, the IAO will;

- Hold system level responsibility for information risk management, as devolved to them by the SIRO.
- System Administrators Vida Healthcare have overall responsibility for the management of risks generated by their information assets.

Caldicott Guardian Function

The Caldicott Guardian will;

- Produce procedures, guidelines and protocols to support staff in the appropriate management of patient information.
- Provide a point of escalation and specialist advice for staff with respect to information sharing, acting as the conscience of the organisation
- Bring to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed and raise concerns about any inappropriate uses made of patient information where necessary.

Data Protection Officer (DPO)

The DPO Will;

- Inform and advise the organisation and its employees about their obligations to comply with the data protection legislation.
- Monitor compliance with the data protection legislation, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, patients etc).

All Staff

All staff, whether clinical or administrative, who create, receive and use data have information governance responsibilities. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

7. TRANSPARENCY

The organisation will;

- Endeavour to make non confidential information about its operations and services available to the public, in line with The Practice's overall commitment to transparency.
- Adopt and maintain clear procedures and arrangements for liaison with the press and broadcasting media.
- Adopt and maintain an Information Rights and Access Protocol and a Freedom of Information Protocol to provide guidance for handling queries from data subjects and the public.

8. PRIVACY AND INFORMATION RIGHTS

Vida Healthcare is committed to the privacy of its patients, staff and the public.

Vida Healthcare will;

- undertake or commission annual assessments and audits of its compliance with privacy and data protection legislation
- adopt and maintain protocol for completion of Data Protection Impact Assessments.
- adopt and maintain protocols to ensure compliance with the Data Protection Act, General Data Protection Regulations, Human Rights Act and the Common Law Duty of Confidentiality.
- establish and maintain protocols for the controlled and appropriate sharing of personal information with other agencies
- ensure that contractual or best practice documents are in place for routine sharing of information between sharing partners.

9. INFORMATION SECURITY

Vida Healthcare will;

- adopt and maintain protocols for the effective and secure management of its information assets and resources.
- scrutinise new systems or services with regards to protecting its information assets and network.
- promote effective information and cyber security practice to its staff through policies, procedures and training.
- establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of information and cyber security.

10. INFORMATION QUALITY AND RECORDS MANAGEMENT

Vida Healthcare will;

- establish and maintain protocols and procedures for information quality assurance and the effective management of records.
- periodically audit / review information quality and records management arrangements.
- Ensure that managers take ownership of, and seek to improve, the quality of information within their services.
- Aim to ensure information quality at the point of collection.
- Set data standards through clear and consistent definition of data items, in accordance with national standards.

11. PROTOCOLS BENEATH THIS POLICY

To ensure that the commitments made in this policy are satisfied, a number of protocols have been developed as below;

- DPS02 Information Rights and Transparency Protocol
- DPS03 Information Disclosure (Including SARs) Protocol
- DPS04 Information Risk and Change Management Protocol
- DPS05 Confidentiality and Information Sharing Protocol
- DPS06 Video, Photography and Audio Recording Protocol
- DPS07 Records Management and Data Quality Protocol
- DPS08 Freedom of Information Protocol
- DPS09 National Data Opt Out Protocol
- DPS10 Online Access Protocol
- DPS11 Information Incident Protocol
- DPS12 Information Security and Cyber Security Protocol

12. APPLICATION AND AUDIT

Compliance with this protocol will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

- ✓ Compliance with this protocol will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.
- ✓ Staff must confirm that they have read and understood this protocol
- ✓ This protocol will be reviewed annually or sooner in the event of significant learning or change
- ✓ This protocol should be read in conjunction with the other protocols in the Data Protection and Security policy suite