iQuda information governance overarching policy

1. Definition of Information Governance

This policy is a statement of iQuda's intentions and approach to fulfilling its statutory and organisational responsibilities towards information governance.

Information governance allows organisations and individuals to ensure that personal information is handled legally, securely, efficiently and effectively in order to ensure the integrity of operations. It additionally enables organisations to put in place procedures and processes for their corporate information that support the efficient location and retrieval of corporate records when and where needed, to assist corporate governance standards.

Information governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information.

The ultimate aim is for an organisation to maintain the confidentiality and security of personal information by helping individual staff members to practice good information governance and be consistent in the way they handle information.

2. Introduction

This policy acts as an overarching policy relating to Information Governance (IG).

Information is a vital asset and plays a key part in corporate governance, service planning, service delivery and performance management. It is therefore important 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.

iQuda recognises the need for an appropriate balance between openness and confidentiality in the management and use of information, thus ensuring we can provide the best possible service by working with other industry level providers and regulatory bodies as appropriate while preserving the confidentiality of personal information about individuals, and commercially sensitive information. iQuda recognises the need to share identifiable personal information with other service providers and agencies in a controlled manner consistent with the interests of the individual and, in some circumstances, in the public interest. At all times, we do this with the prior consent of the individual whose information is in question, where applicable.

iQuda believes that accurate, timely and relevant information is essential to deliver the best quality service. As such it is the responsibility of all staff members to ensure and promote the quality of information as this is often used in decision making processes.

3. Scope

This policy applies to all iQuda staff members, whether permanent, temporary or contracted in (either as an individual or through a third party supplier) and to individuals who are placed at iQuda for work experience.

This policy covers Information Governance matters in relation to all of the information assets of iQuda. There are many types of information asset that iQuda is responsible for, including:

information:
databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;

software assets:
application software, system software, development tools, and utilities;

physical assets:
computer equipment, communications equipment, removable media, and other equipment;

4. Policy Statement

Duties and Responsibilities

IG Lead (also known as the Information Security Manager) – Anthony Jones, Managing Director at iQuda

The IG Lead is responsible for issues relating to personally identifiable data (PID):

1. ensuring that iQuda complies with all legal and ethical requirements relating to the handling of PID
2. supporting and facilitating appropriate information sharing
3. advising on legal and ethical issues relating to processing of PID
4. reporting on information governance requirements and issues to business owners
5. information governance and risk management relating to all information systems
6. encouraging a culture for the safe use of data to advance business purposes
7. providing a focal point for managing information risks and incidents
8. overseeing the management of all information assets
9. developing and maintaining IG policies, procedures and guidance documents
10. ensuring that all information assets are encrypted to meet minimum AES256 Security Standards.
11. responsible for ensuring that iQuda meets our obligations with regards to NHS Information Governance requirements.

In order to develop the organisations processes regarding confidentiality and data protection, the IG Lead:

- works with the internal information governance functions
- delegates information governance work where appropriate
- seeks external advice when needed

When data sharing issues arise, the IG Lead is the main point of contact. A register is maintained of issues relating to data sharing where the IG Lead has exercised their judgement.

CEO – Stephen Macintosh

The CEO is responsible for:

1. supporting and facilitating appropriate information sharing
2. encouraging a culture for the safe use of data to advance business purposes
3. overseeing the management of all information assets

Data Protection Officer – Garth Macintosh

The Marketing and Compliance Officer is responsible for:

1. supporting and facilitating appropriate information sharing
2. encouraging a culture for the safe use of data to advance business purposes
3. reporting on information governance requirements and issues to business owners
4. developing and maintaining IG policies, procedures and guidance documents as delegated by Anthony Jones
5. ensuring compliance with relevant law and legislation including the General Data Protection Regulations 2016 (GDPR)

Service Delivery Director (SDM)– Vincent de Beer

The SDM is responsible for:

1. overseeing IG issues
2. co-ordinating and raising awareness of IG within iQuda
3. monitoring IG risks.
4. Alerting the IG Lead when we are at risk of breaching any confidentiality.
5. ensuring that the IG policies are adhered to within their teams
6. reporting on data incidents when appropriate
7. encouraging their staff to develop their understanding of IG and to apply the principles in everything they do
8. ensuring that all information assets are encrypted to meet minimum AES256 Security Standards if assigned the responsibility of preparing the asset for use.

Technical Director – James Watson

The technical director is responsible for:

1. maintaining the iQuda IT network in line with all applicable policies.
2. ensuring risks are well addressed when making changes to the network.
3. ensuring the IT network is well designed and maintained.
4. overseeing IG incidents within the technical department.
5. ensuring disaster recovery procedures are well designed and reliable from a technical perspective.

Staff and temporary employees

All staff members, whether permanent, temporary or contracted-in (either as an individual or through a third-party supplier), are responsible for:

1. ensuring that they are aware of the requirements incumbent upon them
2. ensuring that they comply with these policies on a day-to-day basis.
3. completing mandatory information governance training
4. ensuring that all information assets are encrypted to meet minimum AES256 Security Standards if assigned the responsibility of preparing the asset for use.
5. ensuring that breaches or untoward incidents are reported using the Incident Report procedure
6. ensuring that no unauthorised changes are made to information assets

The Policy: Overview

There are 4 key interlinked strands to the IG Policy:

- Confidentiality
- Legal Compliance and corporate governance;
- Information Security;
- Data protection

4.1 Confidentiality *(See Q200 iQuda Staff confidentiality code of conduct)*

iQuda regards all personal data about individuals and commercially sensitive data as confidential, and takes steps to ensure that all staff respect the confidentiality of personal information. This includes appropriate training for all staff working in the organisation, to ensure that staff respect confidentiality, and also know when it is appropriate to share information.

4.2 Legal Compliance and Corporate Governance

Confidential data must be processed in accordance with the General Data Protection Regulations 2018 and the Common Law Duty of Confidentiality.

4.3 Information Security *(See Q201 iQuda Information Security Policy)*

Information Security is fundamental to the operation of iQuda due to the confidential data it accesses and processes, and the reliance on information systems to process data. iQuda relies on password protection to maintain security of information. Please refer to iQuda IT acceptable use, remote access, portable media and passwords policies.

4.4 Information Quality Assurance

All staff members are expected to take ownership of, and seek to improve, the quality of information used within their business area.

4.5 Data protection *(See QGDPR iQuda GDPR Policy)*

Article 5 of the GDPR requires that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5 (2) requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

iQuda intends to comply with the above requirements and will implement appropriate mechanisms to ensure continued compliance.

5.0 Enforcement

This policy will be enforced by the Executive Team and Data Protection Officer. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. In the event of a policy breach that leads to a data breach in violation of the GDPR, the Data Protection Officer may need to report the breach to the Information Commissioners Office (the ICO). Please refer to the QGDPR iQuda GDPR Policy and the QDBRP iQuda Data Breach Response Policy for more information.

6.0 Policy review

This policy will be reviewed at least annually. The policy will be reviewed before this timeframe if the relevant supervisory authority releases new legislation or guidance.