QUESTA
PSYCHOLOGICAL SERVICES

INFORMATION SECURITY POLICY

Company No 12911052
www.questapsych.com
admin@questapsych.com
02381 924877

Registered office:
Exchange House
Cross Street
Newport PO30 5PZ

Purpose

Information that's collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation, as well as possible judgements being made against Questa.

Questa undertakes assessment, diagnosis and therapy for a range of mental health conditions. In this context, acutely sensitive client (patient) data is recorded, stored and, where appropriate, shared amongst members of the company and associates.

This document is to provide the high-level outline of, and justification for, Questa's information security controls.

Objectives

Questa's security objectives are that:

- our information risks are identified, managed and treated according to an agreed risk tolerance
- our authorised users can securely access and share information in order to perform their roles
- our physical, procedural and technical controls balance user requirements and security
- our contractual and legal obligations relating to information security are met
- our training activity considers information security
- individuals accessing our information are aware of their information security responsibilities
- incidents affecting our information assets are resolved and learnt from to improve our controls

Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used at Questa, in all formats. This includes information processed by other organisations in their dealings with Questa.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Questa information and technologies. This includes external parties that provide information processing services to Questa.

Questa acts in the role of "data controller" and, as such, is registered with the ICO.

Compliance monitoring

Compliance with the controls in this policy will be monitored by the Directors of Questa.

Review

A review of this policy will be undertaken annually or as required.

Policy Statement

It is Questa's policy to ensure that information is protected from a loss of:

- confidentiality – information will be accessible only to authorised individuals
- integrity – the accuracy and completeness of information will be maintained
- availability – information will be accessible to authorised users and processes when required

Questa will implement an Information Security Management System based on certified standards as required. Questa will be mindful of the approaches adopted by its stakeholders, including commercial partners.

Questa will adopt a risk-based approach to the application of the following controls:

1. INFORMATION SECURITY POLICIES

A set of lower-level controls, processes and procedures for information security will be defined, in support of the high-level Information Security Policy and its stated objectives.

2. HUMAN RESOURCES SECURITY

Questa's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff. Poor or inappropriate behaviour will be addressed.

Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

3. ACCESS CONTROL

Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed, and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. The separation of duties will be implemented, where practical.

4. CRYPTOGRAPHY

Questa will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

Client (patient) data is stored and retrieved from a cloud based medical software system called WriteUpp with servers located within the EU in Dublin so as to be GDPR compliant. WriteUpp is ISO27001 certified; ISO27001 is a globally recognised information governance and security standard. WriteUpp's systems and processes comply with this standard and are audited annually to ensure continued compliance.

6. OPERATIONS SECURITY

If necessary, records are maintained locally by practitioners. Questa will ensure the correct and secure operations of information processing systems. This will include:

- documented operating procedures

- the use of formal change and capacity management
- controls against malware
- defined use of logging
- vulnerability management

7. COMMUNICATIONS SECURITY

Messages sent via the integrated email service in WriteUpp are encrypted using TLS which is a cryptographic protocol that provides end-to-end security of data sent between applications over the internet. TLS uses a combination of symmetric and asymmetric cryptography, as this provides a good compromise between performance and security when transmitting data securely. Data is encrypted and decrypted with a secret key known to both sender and recipient; typically 256 bits in length.

Questa will maintain network security controls to ensure the protection of information within its networks. Questa will also provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities. This is in line with the classification and handling requirements associated with that information.

8. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to reduce any risks identified will be implemented where appropriate.

9. INFORMATION SECURITY INCIDENT MANAGEMENT

Guidance will be available on what constitutes an information security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. The appropriate action to correct the breach will be taken, and any learning built into controls.

10. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Questa will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters. This is to ensure their timely recovery in line with documented business needs. This will include appropriate backup routines and built-in resilience.

Through WriteUpp, client (patient) data is replicated in real-time to two separate physical locations and then to four additional locations within those physical locations.

Questa is dependent upon WriteUpp's business continuity plans being maintained and tested in support of this policy. Business impact analysis will be undertaken, detailing the consequences of:

- disasters
- security failures
- loss of service
- lack of service availability

11. COMPLIANCE

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

Currently this includes:

- data protection legislation
- the Information Commissioner's Office with particular regard to GDPR
- Questa's contractual commitments

Questa will use a combination of internal and external audits to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures. This will include:

- IT health checks
- internal checks on staff compliance
- returns from Information Asset Owners

Review of this document: annually

Next review date: November 2025