

Information Governance v4.3

standards module



The voice of technology
enabled care



Description

“Information Governance is often seen simply as a way of securing information and data belonging to an organisation, its service users, carers and employees - and keeping it private. All technology enabled products and services should see 'Governance' as a way to harness the value of that information to enable better service outcomes and improved care delivery whilst minimising the risk of disclosure.”

Dave Foster

Dave Foster, Chair, TSA Technology Standards Board



Information is a vital asset, both in terms of the management of individuals and in the efficient organisation of services and resources. Information governance (IG) provides a framework that ensures personal and sensitive information relating to service users, carers and employees is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.



Key Outcomes

- Organisations will recognise and be able to articulate the need for a clearly formulated balance between openness and confidentiality in the management and use of information
- Everyone involved in service delivery will be aware of their responsibilities to ensure and promote quality of information and will seek to actively use it in decision-making processes
- Information sharing between professionals and across organisational boundaries will be improved, in a controlled manner consistent with the interests of the service user

The Audit Process

The Audit Process will seek robust evidence that the key outcomes have been met.

As a minimum, TEC Quality certified organisations **must:**

Demonstrate an understanding and application of processes supporting the three most crucial components of information security: Confidentiality, Integrity and Availability (CIA).

Demonstrate awareness of and compliance with relevant legislation, regulatory guidance and best practice in relation to information governance.

Have a UK GDPR policy, which also includes data retention.

Have standardised systems for the inputting, checking and maintenance of accurate and up-to-date customer/user information, which shall be checked at least annually.



Have procedures and mechanisms in place that ensure customers, service users and carers know how their personal information will be used and which enable customers, service users and carers to access this information.

Have data sharing agreements with key partners in place to ensure that people can receive proportional support without duplication.

Provide evidence that data protection breaches are reported via defined processes and that opportunities for learning are identified and shared to minimise the risk of them reoccurring.

Provide evidence that Data Privacy Impact Assessments* (DPIA's) are considered and when undertaken are in line with the ICO's 'privacy by design' approach.

Have written procedures to manage the organisational and staff use of social media.

Provide evidence that all staff understand their roles and responsibilities in relation to information governance.

*DPIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information.

Have written procedures in place to ensure system access and data security are maintained e.g. password access protections, anti-virus and anti-malware software, secure sending of emails, secure encryption of electronic removable media and portable computing devices and transport/storage of paper records.

Provide evidence that the physical security of IT assets and information is maintained to recognised industry standards and follows vendors recommended processes.

Provide evidence that secure storage of and access to paper records is in place.

Be able to demonstrate robust Cyber Security for their organisation.

Compliance with Cyber Essentials (self-certificated) or DSPT as a minimum.

Demonstrate awareness of the risks presented by cyber-attacks, and that through informed decisions, a risk-based approach to cyber security and insurance has been undertaken.



Evidence might include:

- Data Protection and Confidentiality Policy
- Freedom of Information Policy
- Incident Reporting Policy
- Consent Policy
- Whistleblowing Policy

- Staff training records
- Information quality and records management audits
- Information Sharing Policy
- Information Asset Owners in place

- For organisations providing clinical services:
 - Information Governance Statement of Compliance (IGSoC) minimum level 2
 - Named Caldicott Guardian

www.tecquality.org.uk

TEC Quality is the organisation set up to develop and run the Quality Standards Framework (QSF) - a set of outcome based standards developed in partnership with key stakeholders across the TEC sector. TEC Quality audits and certifies organisations against these standards.

Whilst QSF is the intellectual property of the TSA, TEC Quality has full autonomy and sector-wide support to administer the QSF standards.