Technical and Organisational Measures

Last updated: February 2024

This policy outlines the Technical and Organisational Measures implemented across Talking Medicines for secure and compliant processing of data. This ensures the ongoing confidentiality, integrity, and availability of Talking Medicines Services.

Talking Medicines adopt appropriate technical and organizational measures reflective of current best industry practice and technological development to protect Personal Data against accidental or unlawful destruction or accidental loss (including deletion), alteration (including corruption), unauthorized disclosure, use or access and against all other unlawful forms of Processing.

1. Standard security controls with reference to Article 32 of the General Data Protection Regulation ("GDPR") which requires Data Controllers and Data Processors to implement technical and organizational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data

Measures of pseudonymisation and encryption of personal data

All data is stored within Azure blob, Azure Databricks and Azure SQL Server storage, which is natively encrypted at rest and in transit.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Talking Medicines has personnel responsible for oversight of security and privacy. It has an appointed Chief Data Officer, Data Privacy and Compliance Manager. This is coupled with a Data Privacy & Security Subcommittee and a Quality Subcommittee that meets quarterly to discuss data privacy, artificial intelligence and security risks which are further managed through to the Company risk registers, which is reported at Board level.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Talking Medicines hosts its solutions within Microsoft Azure with both the primary and secondary datacentres. Azure is hosted in Microsoft's data centres around the world, and offers best industry practice performance, scalability, security, and service levels.

Microsoft has applied state-of-the-art technology and processes to maintain consistent and reliable access, security, and privacy for every user. Azure has built-in capabilities for compliance with a wide range of regulations and privacy mandates.

Microsoft Azure, Dynamics 365, and other Microsoft online services undergo regular independent third-party audits for ISO/IEC 27001 compliance. The Azure ISO/IEC 27001 certificate covers Azure, Dynamics 365, select Microsoft 365, and Power Platform online services.

Talking Medicines provides the following service levels.

- Recovery Point Objective (RPO): < One hour.
- Recover Time Objective (RTO): < Six hours during Core Business Hours.

Talking Medicines utilise Microsoft Azure's standard backup and geo-replication facilities. The following provides further technical details on the backup services that we utilise.

SQL Databases:

- Point-in-time Restore over the last 35 days.
  This is achieved by
  - Full database backups are created weekly, differential database backups are created every 24 hours, and transaction log backups are created every 5 - 10 minutes, with the frequency based on the compute size and amount of database activity.
  - Backups are geo-replicated offsite to the secondary UK datacentre.
- Long Term backups
  - These are stored - Weekly for 3 months; Monthly for 15 months; Yearly for 7 years.
  - Backups are geo-replicated offsite to the secondary UK datacentre.
- All back-ups are encrypted at rest using Azure managed keys.

Azure Storage Accounts (Blob storage):

- Data is Geo-replicated to the secondary UK Data centre using Geo-redundant storage.
- Geo-redundant storage is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year by replicating data to a secondary region that is hundreds of miles away from the primary region (but still within the UK).
- All data is first replicated with locally redundant storage (LRS). An update is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region using GRS. When data is written to the secondary location, it's also replicated within that location using LRS.
- Azure Storage encryption is used to encrypt all data at rest.
- All files stored with Azure Storage utilise "Soft-deletion" where by if they are deleted or overwritten a snapshot is taken and is available for 365 days should it need to be recovered.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Software security penetration testing is conducted periodically by an independent third party supplier. All issues found are triaged, risk assessed and resolved by the team according to their potential impact.

2. Security Controls: Access

Talking Medicines maintains appropriate controls for requesting, approving, granting, modifying, revoking and revalidating user access to systems and applications.

Access Management

All data is stored within Microsoft Azure blob, Microsoft Azure Databricks and Microsoft Azure SQL Server storage, which is natively encrypted at rest and in transit.

Access to this data is restricted to Talking Medicines Azure Active Directory (AD) accounts which have been explicitly granted authorisation to the data. Azure AD provides the central authentication mechanism, including the use of multi-factor authentication, to secure access. Administrative accounts require specific and informed review before given access rights.

Data access is restricted to only those individuals that require access as part of their role. Users have the minimum access required to perform job duties.

Password Management

Talking Medicines employs strong password management throughout the Company with a password management procedure. The 1Password password management system is mandatory for all employees.

3. Security Controls: Physical Security

Physical Access Controls and Environmental Security

Talking Medicines relies on the physical, environmental and infrastructure controls of Microsoft. Talking Medicines periodically reviews certifications and third-party attestations provided by Microsoft relating to the effectiveness of its data centre controls.

Access to Talking Medicines offices (the only physical premises) is controlled and based on business necessity and the individual's role and relationship to Talking Medicines.

Talking Medicines offices are managed offices and are secured by access control systems. Visitors who require access to Talking Medicines offices must enter through a staffed and/or main facility entrance. Visitors must register their arrival and exit. Visitors must produce a current, government issued form of identification to validate their identity.

The managed offices use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted.

4. Security Controls: Information Security

Ensuring events logging

Talking Medicines maintains application and infrastructure security audit logs. Talking Medicines send logs into a central Azure Log monitor solution. Azure Log monitor alerts are then created to raise any issues identified.

Application errors, in the browser, are captured and logged by Sentry.

Anti-Malware

ESET Malware Protection & Internet Security implemented on local machines.

Threat and Vulnerability Management

Talking Medicines have a vulnerability and patch management process for information systems, infrastructure, and networks to regularly identify and track vulnerabilities through the lifecycle. The supporting infrastructure or networks are scanned for vulnerabilities on an ongoing basis. Vulnerabilities are tracked and remediated with appropriate risk mitigation requirements through documentation. All system, software, and network components are protected from known vulnerabilities by installing applicable third-party supplied security patches. The frequency of patching is ongoing.

Patch Management

Talking Medicines employ an Azure managed patch and upgrade policy for Azure services. Custom built software is managed to alert and manage patches on third party components.

High and Critical patches are applied as soon as they are highlighted by either monitoring tools or the software build process. The impact of the patches on software and systems is tested within development environment and remediations are made there. Patches and any remediations are passed to staging environment to be tested as one before being deployed to production environment.

Network Security

Talking Medicines have an established policy around wireless network security policy for protecting wireless network environments from unauthorized traffic, personnel, and devices.

Removable Media

No removable media is utilised.

Cybersecurity Incident Response

Talking Medicines maintains a Security Incident Response Procedure. This procedure details the requirements to:

- review and test the incident response plan
- the requirement to maintain a record of all security incidents
- the requirement to have an escalation process
- includes coordination with internal stakeholders and relevant authorities such as law enforcement agencies, providing legally admissible chain-of-custody management processes, and forensic analysis techniques

Recovery and back up

Talking Medicines hosts its solutions within Microsoft Azure with both the primary and secondary data centres. Azure is hosted in Microsoft's data centres around the world, and offers best industry practice performance, scalability, security, and service levels.

Microsoft has applied state-of-the-art technology and processes to maintain consistent and reliable access, security, and privacy for every user. Azure has built-in capabilities for compliance with a wide range of regulations and privacy mandates.

Microsoft Azure, Dynamics 365, and other Microsoft online services undergo regular independent third-party audits for ISO/IEC 27001 compliance. The Azure ISO/IEC 27001 certificate covers Azure, Dynamics 365, select Microsoft 365, and Power Platform online services.

Talking Medicines provides the following service levels.

- Recovery Point Objective (RPO): < One hour.

- Recover Time Objective (RTO): < Six hours during Core Business Hours.

Talking Medicines utilise Microsoft Azure's standard backup and geo-replication facilities. The following provides further technical details on the backup services that we utilise.

SQL Databases:

- Point-in-time Restore over the last 35 days.
  This is achieved by
  - Full database backups are created weekly, differential database backups are created every 24 hours, and transaction log backups are created every 5 - 10 minutes, with the frequency based on the compute size and amount of database activity.
  - Backups are geo-replicated offsite to the secondary UK datacentre.
- Long Term backups
  - These are stored - Weekly for 3 months; Monthly for 15 months; Yearly for 7 years.
  - Backups are geo-replicated offsite to the secondary UK datacentre.
- All back-ups are encrypted at rest using Azure managed keys.

Azure Storage Accounts (Blob storage):

- Data is Geo-replicated to the secondary UK Data centre using Geo-redundant storage.
- Geo-redundant storage is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year by replicating data to a secondary region that is hundreds of miles away from the primary region (but still within the UK).
- All data is first replicated with locally redundant storage (LRS). An update is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region using GRS. When data is written to the secondary location, it's also replicated within that location using LRS.
- Azure Storage encryption is used to encrypt all data at rest.
- All files stored with Azure Storage utilise "Soft-deletion" where by if they are deleted or overwritten a snapshot is taken and is available for 365 days should it need to be recovered.

5. <u>Security Controls: Data</u>

Data Retention

Talking Medicines maintains a Data Retention Policy setting out the retention periods for various types of data based on legal requirements, justified interests of Talking Medicines and the purposes of collection.

Talking Medicines has implemented data privacy by design principles, including but not limited to, privacy impact assessments.

Data Destruction

Talking Medicines maintains a Data Destruction Policy which acts in accordance with Customer contractual arrangements and considers legal requirements, justified interests of Talking Medicines and the appropriate method of destruction in the ordinary course of business.

Data Classification

We have data handling processes in place, constantly assessing the critical data point interactions, assessing and mitigating risks to remain in control. This is done through a sensitivity and confidentiality assessment. There are requirements for this to be labelled, stored and protected appropriately.

Code and Document change control is managed through performing risk assessments on a continuous basis – deviations are tracked and documented.

Data Encryption

All data is stored within Azure blob, Azure Databricks and Azure SQL Server storage, which is natively encrypted at rest and in transit.

Clear Desk

Talking Medicines adopts a Clear Desk policy.

6. Security Controls: Governance

Talking Medicines is governed through monthly Board meetings which discuss and detail corporate strategy, authorisation or business plans, financial objectives and ensure that the business has the resources, structures and governance in place to pursue the mission and vision, with proper regard for regulatory and compliance items.

There are three established governance bodies that run quarterly to oversee Company activities:

(1) The Data Privacy & Security Subcommittee (established September 2022). The Data Privacy and Security Subcommittee was established as the governance vehicle to challenge Talking Medicines to be forward thinking and accommodating with changes to regulatory and legal landscapes.

(2) The Quality Subcommittee (established 2018). The Quality Subcommittee is the governance vehicle for process and patient safety. The aim of the Quality Subcommittee is primarily to track and control the quality and security of medicines data from Patients, Customers and Talking Medicines point of view.

(3) The Governance Subcommittee (established 2024). The Governance Subcommittee is an internal subcommittee established to govern the governance structure and decisions of Talking Medicines.

Gaining trust and integrity through data quality and security are critical to the success of Talking Medicines. The ethos of Talking Medicines is to ensure that quality runs through the core of the business which is delivered through data governance and assurance.

Talking Medicines are registered with the ICO as a Data Controller (reference number: Reference: ZA079728). Talking Medicines are the Data Processor for Customer Data. The Company works to an agreed internal process for good information governance. Talking Medicines take data handling, security and protection exceptionally seriously and are constantly reviewing and improving internal processes.

Data Protection Impact Assessments are carried out for high risk processing activities and Talking Medicines maintains records of its processing activities.

Risk Management

Risk is managed through the Company Risk Register. The Risk Register is an articulation of the key risks impacting the business. It is used to inform decision making, provide assurance over actions being taken to manage key risks and to inform Board level risk management planning and mitigation activities.

Quality Control processes are in place for identifying, monitoring and challenging quality. We have data handling processes in place, constantly assessing the critical data point interactions, assessing and mitigating risks to remain in control. Code and Document change control is managed through performing risk assessments on a continuous basis – deviations (changes) being tracked and documented.

Talking Medicines have an in-house annotation team who have created gold-standard training data based on healthcare voices. Resulting in pre-trained, “ready to use” models. Building and managing an internal team of Annotators has been an essential part of ensuring model accuracy through the use of our proprietary Gold-standard training data.

Information Security Policy Management

Talking Medicines maintains a documented, approved, and communicated information security policy that describes how Talking Medicines manages information security. Talking Medicines have a risk management process to identify, assess, monitor, and respond to information security risks.

Talking Medicines information security practices are aligned to ISO27001 with controls implemented in line with our risk assessment of any threats and vulnerabilities. Talking Medicines assess adherence to information security practices, which is overseen by the governance vehicles detailed above.

Third party assessments

Talking Medicines use third parties that adhere to strict compliance and security guidelines, including but not limited to data requirements, stability, security and more. Third parties are reviewed on both an ongoing and periodical basis by appropriate personnel.