



Data Management Policy for Kelvin

This policy summarises the procedures Machine Medicine Technologies Ltd (MMT) follows in order to maintain industry standard data security for the Kelvin platform.

1. Regulatory Standards

1.1. GDPR & HIPAA

Our data management procedures were created to be compliant with the EU and UK General Data Protection Regulation (GDPR) and the U.S. Health Insurance Portability & Accountability Act (HIPAA). All members of the Machine Medicine workforce are required to undergo GDPR and HIPAA awareness training before working with sensitive information. Machine Medicine also complies with ISO 27001, an information security management system (certificate number IS 744149).

2. Hosting Provider

2.1. Cloud Provider

Kelvin is hosted by Google Cloud Platform (GCP). Google and GCP have high standards with respect to privacy, as well as gold standard processes with respect to network security and physical design standards.

2.2. Contract

Machine Medicine Technologies has a business associate agreement with GCP, in accordance with HIPAA regulations.

2.3. Availability

The availability and integrity of the infrastructure underpinning Kelvin are constantly being monitored using cloud provider tools. If a loss of service were to occur MMT would be alerted immediately.

2.4. Data residency

There are two separate versions of Kelvin operating in different regions:

USA - Patient data uploaded to cloud.machinemedicine.com is stored in the USA.

EU - Patient data uploaded to cloud.machinemedicine.eu will be stored in the EU.

Patient data is never transmitted between regions.

3. Platform Security

3.1. Connections

Transfers to, from or within Kelvin are made over Secure Socket Layer (SSL) connections.

Transfers within Kelvin have the additional protection of Transport Layer Security 1.2 (TLS1.2). Cloud provider firewalls restrict open ports to a minimum. Developer access to the Kelvin backend has multiple safeguards including multi-factor authentication, cloud provider session management, and Internet Protocol (IP) whitelisting.

3.2. Encryption

Advanced Encryption Standard 256 (AES-256) is used to encrypt all data held on Kelvin, as well as all data held on devices used by members of the Machine Medicine workforce.

3.3. Account Protection

User accounts for Kelvin require secure passwords. An account will be locked if three failed login attempts are made and can only be unlocked through a link sent to the user's email address. Accounts are automatically logged out of Kelvin after 15 minutes of inactivity, and must re-enter their password to access their data.

3.4. Vulnerability Prevention

Intrusion Prevention and Detection systems constantly monitor Kelvin for malicious attacks. All software used by Kelvin is on vendor supported versions, and a configuration and patch management system is in place to further minimise risk. Kelvin undergoes Vulnerability Assessments and Security Penetration Testing.

3.5. Antivirus

Kelvin runs on Ubuntu servers, the typical industry standards for delivering secure services from Ubuntu servers do not include the use of antivirus. All computers used by Kelvin developers have antivirus installed and updated on a regular basis.

4. Data Security

4.1. Processing

All data entered into Kelvin is processed, stored and backed up automatically. This eliminates the possibility of human error causing any destruction of data. Video data can be uploaded to Kelvin in any of the following formats: MP4, MOV, AVI, WEBM.

4.2. Physical Media

All Kelvin data is stored and managed using cloud services. Physical storage media such as flash drives or DVD ROMs, are never used to store or transport patient data.

4.3. Backups

Every hour data is automatically backed up. This means that even in the event of a catastrophic failure of the main Kelvin server, Machine Medicine Technologies will be able to restore data from more than one backup.

4.4. Monitoring

All activity on the Kelvin platform, including backups and backend developer access, is monitored and recorded using cloud provider services and other secure tools.

4.5. Access

At any time, users with sufficient access permissions can download their data from Kelvin in universal file formats.

Videos are downloadable as MP4 files. All other data, including analytical results, are downloadable as CSV or JSON files.

4.6. User Accounts & Permissions

A user is invited to create an account through their organization. By default, user accounts are created with the minimum level of access but are able to request increased access should it be required.

4.7. Assessment Archiving

Users can 'archive' their assessments at any time however the assessment will not be deleted from the database once uploaded to the Kelvin platform. The assessment will be removed from the user's dashboard but will be accessible to MMT.