KELVIN

Machine Medicine

CE KELVIN-PD is regulated by the MHRA and is CE marked for conformance as a medical device

Data Management Policy for KELVIN-PD

This policy summarises the procedures Machine Medicine Technologies Ltd (MMT) follows in order to maintain industry standard data security for the KELVIN-PD platform. This document is intended for an external audience; the full set of MMT data management procedures spans numerous documents which go into a far greater level of detail, and can be obtained upon request.

1. Regulatory Standards

1.1. GDPR & HIPAA

Our data management procedures were created to be compliant with the General Data Protection Regulation (GDPR) and the 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.

1.2. Medical Device Regulation

KELVIN-PD is a medical device and as such has been designed in compliance with the European Union Medical Device Regulation 2017/745, the European Medical Device Vigilance System 2.7.1, as well as other relevant International Organization for Standardization (ISO) specifications[1].

1.3. Quality Management System

Machine Medicine Technologies operates a quality management system designed in compliance with ISO 13485.

2. Hosting Provider

2.1. Amazon Web Services

[1] The KELVIN-PD meets the following ISO specifications: 62304, 62366, 14155, 1041, 15223, 14971, 80001.

KELVIN-PD is hosted by Amazon Web Services (AWS), the largest cloud services provider in the world. AWS have high standards with respect to privacy[2], as well as gold standard processes with respect to network security[3] and physical design standards[4].

2.2. Contract

Machine Medicine Technologies has a business associate contract with AWS, in accordance with HIPAA regulations.

3. Platform Security

3.1. Connections

Transfers to, from or within KELVIN-PD are made over Secure Socket Layer (SSL) connections. Transfers within KELVIN-PD have the additional protection of Transport Layer Security 1.2 (TLS1.2). Developer access to the backend of KELVIN-PD has multiple safeguards including multi-factor authentication, Secure Shell (SSH) keys and Internet Protocol (IP) whitelisting.

3.2. Encryption

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

3.3. Account Protection

User accounts for KELVIN-PD require secure passwords which must be changed every six months. 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. If a user is inactive for 30 minutes they are automatically logged out and must re-enter their password to access their data.

4. Data Security

4.1. Processing

All data entered into KELVIN-PD 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-PD in any of the following formats: MP4, MOV, AVI, WEBM.

4.2. Backups

Every hour data is automatically backed. Backups are held in multiple locations within the European Union and the United States. This means that, even in the event of a catastrophic failure of the main KELVIN-PD server, Machine Medicine will be able to restore all data from more than one backup.

4.3. Monitoring

[2] Click here to read more about how AWS ensures data privacy

[3] Click here to read more about how AWS ensures cloud security

[4] Click here to read more about how AWS designs their data centers

All activity on the KELVIN-PD platform, including backups and backend developer access, is monitored and recorded using services from AWS and other secure tools.

4.4. Access

At any time, users can download their data from KELVIN-PD in universal file formats. Videos are downloadable as MP4 files. All other data, including analytical results, are downloadable as CSV or JSON files.