SilverCloud

MAKING SPACE FOR HEALTHY MINDS

Technical & Organisational Security Measures

June 2019

1. Organisation of information security

SilverCloud Health Ltd (SilverCloud) has a documented Information Security Management System (ISMS) covering the areas of technical and organisational security described in this document and holds ISO 27001:2013 and Cyber Essentials certifications. ISO 27001:2013 audits are conducted by a thirdparty twice per year as part of our on-going compliance programme.

SilverCloud has formal documented information security policies approved by management and has formally assigned and documented roles and responsibilities for information security and data protection.

Information security risk management is a core part of the overall ISMS. Risk management includes maintenance of a risk register and risk treatment plan.

2. Suppliers

SilverCloud uses third-party suppliers to provide its services. Suppliers are subject to information security risk assessment and must have an appropriate contract in place, including suitable clauses addressing data protection.

Key suppliers are Armor Defense Ltd (hosting in UK) and Amazon Web Services (hosting in Ireland). These providers have relevant security certifications, outlined below:

Armor - see https://www.armor.com/certifications/

- ISO 27001:2013
- SSAE SOC 1 / SOC 2 / SOC 3
- HITRUST CSF

Amazon Web Services - see https://aws.amazon.com/compliance/programs/

- ISO 27001:2013
- SSAE SOC 1 / SOC 2 / SOC 3

A list of suppliers is set out at https://www.silvercloudhealth.com/privacy/platform#subprocessors

3. Asset management

SilverCloud maintains a register of key physical and informational assets, including owners. The company has an information classification and labelling scheme. Customer data is treated as Confidential, while patient data is treated as Restricted, the highest classification in our scheme.

4. Human resources security

Background checks are performed for new personnel. Where relevant, staff undergo vetting for work with children or vulnerable adults. All staff have an obligation to uphold confidentiality under the conditions of employment and company policies. Information security training and on-going awareness information is provided to personnel.

5. Physical & environmental security

The SilverCloud platform is hosted with secure hosting providers that offer a high level of physical and environmental security. For the primary hosting provider Armor, in addition to the physical access controls maintained for entry into the building and the raised floor space (multi-factor authentication using badges and biometrics for access throughout the facility, 24 hour guards, video monitoring), Armor has installed, maintains and monitors its own multi-factor physical access controls and its own video surveillance for its dedicated cage. All visitors are escorted at all times within the datacentre and no visitors are allowed at all inside its dedicated cage.

SilverCloud's office headquarters have appropriate physical security including building security guard and CCTV, access-controlled doors, clean desk / clear screen policy, CCTV monitoring and additional physical access control of server room.

6. Communications & operations security

SilverCloud has antivirus products installed on office computers and hosting servers, with automatic updates. Security patches are regularly installed. Firewalls are in place to control unauthorized access. The production hosting environment is monitored by the hosting provider security operations centre team, who operate intrusion detection systems. SilverCloud ensures vulnerability scans are performed monthly and penetration tests at least once per year.

Encryption is used to protect data stored on office and portable computers, and also to protect data at rest and in transit to the SilverCloud platform.

7. Access controls

There is documented access control policy covering authorisation of access rights to systems, procedure for new personnel, changes of role, and terminations. Access is reviewed at least annually. Unique accounts are assigned to individuals and sharing is not permitted by policy. Passwords must meet the documented policy, and default passwords are changed.

The SilverCloud platform requires passwords to meet documented complexity requirements, forces re-authentication after inactivity, and disables access temporarily after a number of unsuccessful logon attempts.

8. Information security incident management

SilverCloud has a documented incident response policy, approved by management, setting out responsibilities, classification of incidents, procedures for incident handling, and requirements for notifying customers. The incident response process is tested at least annually.

9. Business continuity management

SilverCloud has documented business continuity and disaster recovery plans for the SilverCloud platform. The business continuity process is tested at least annually. Risks related to business continuity are reviewed at least annually and results of reviews and tests are used to update plans as necessary.