Security Policy: last updated 9th August 2019

All operational data within the SCR system is encrypted both at rest and in transit using industry standard techniques. Transit is handled by the secure transport protocol and the database platform manages encryption at rest with our provided keys; these keys are subject to the same security as detailed below.

Personal information stored within the profiles in the application are subject to a second layer of encryption that includes the organisation as a context. No user of the SCR software has the ability to decrypt data for the profiles that aren't explicitly a member of the organisation and granted permission to do so.

Staff members at SCR are unable to access this data without explicit permission being granted in a support session; any time this scenario is taking place you will be notified within the application that a support session is active. Even technical staff with access to the database for operational reasons cannot access this data.

Keys are managed in the AWS cloud using hardware security modules, this enables us to guarantee that no member of staff from SCR or AWS would ever be able to retrieve plaintext keys from the service. This follows that any access to the service to decrypt profile data is fully tracked and audit record is kept. Security and quality controls in AWS Key Management Service have been validated and certified by the following compliance schemes:

* AWS Service Organisation Controls (SOC 1, SOC 2, and SOC 3) Reports. You can download a copy of these reports from AWS Artifact (https://aws.amazon.com/artifact/).
* PCI DSS Level 1. For more details on PCI DSS compliant services in AWS, you can read the PCI DSS FAQs (https://aws.amazon.com/compliance/pci-dss-level-1-faqs/).
* ISO 27001. For more details on ISO 27001 compliant services in AWS, you can read the ISO 27001 FAQs (https://aws.amazon.com/compliance/iso-27001-faqs/).
* ISO 27017. For more details on ISO 27017 compliant services in AWS, you can read the ISO-27017 FAQs (https://aws.amazon.com/compliance/iso-27017-faqs/).
* ISO 27018. For more details on ISO 27018 compliant services in AWS, you can read the ISO-27018 FAQs (https://aws.amazon.com/compliance/iso-27018-faqs/).
* ISO 9001. For more details on ISO 9001 compliant services in AWS, you can read the ISO-9001 FAQs (https://aws.amazon.com/compliance/iso-9001-faqs/).
* FIPS 140-2. The AWS KMS cryptographic module running firmware version 1.4.4 is validated at FIPS 140-2 Level 2 overall with Level 3 for several other categories, including physical security. For more details, you can view the FIPS 140-2 certificate for AWS KMS HSM (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139) along with the associated Security Policy (https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3139.pdf).
* FedRAMP. You can get more details on AWS FedRAMP compliance at FedRAMP Compliance (https://aws.amazon.com/compliance/fedramp/).
* HIPAA. For more details, you can visit the HIPAA Compliance page (https://aws.amazon.com/compliance/hipaa-compliance/).