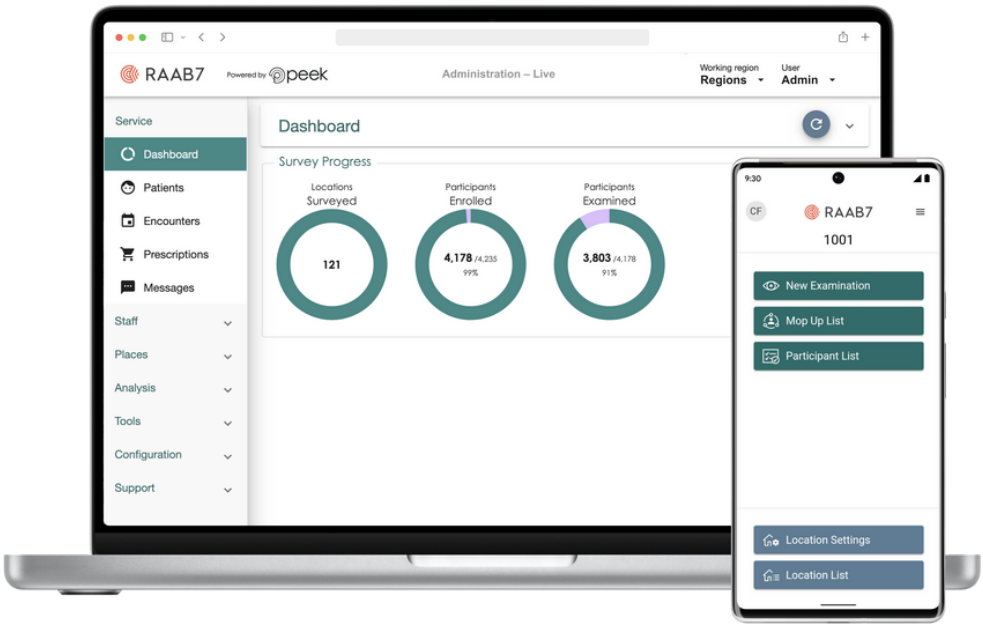
RAAB7 | Rapid Assessment of Avoidable Blindness

# Data security and data protection

RAAB7 is the latest version of the Rapid Assessment of Avoidable Blindness survey, developed by Peek Vision and the London School of Hygiene & Tropical Medicine's International Centre for Eye Health. Robust data security and data protection are an integral part of RAAB7's design. Survey data is processed in line with the most stringent data protection regulations. The RAAB7 software is secure and we follow global best practice in data security to ensure information is kept safe at all times.



# Cloud Security

## AWS Cloud security

RAAB7 is hosted on the Amazon Web Services (AWS) Cloud - one of the most secure and well-established cloud computing environments available today. The core AWS infrastructure is built to satisfy the security requirements of healthcare providers, military, global banks, and other high-sensitivity organisations.

- All RAAB7 data on the AWS Cloud is securely stored in AWS data centres located in Germany or India only. These are state of the art facilities with robust physical and digital security measures to protect against manmade and natural risks. Data centres undergo independent third-party audit inspections to confirm security and compliance.

**Take a virtual tour of an AWS data centre to learn more about the security measures in place to protect RAAB7 data.**

- AWS provides assurance of cloud security and privacy controls through the AWS Compliance Program. This provides certified assurance of the robust controls in place to maintain security and compliance in the cloud. Certification and attestations include ISO 27001, ISO 27017 and SSAE 18 SOC 1- 3 service audit reports.

**View further details on the AWS Compliance Program in place to ensure stringent cloud security.**

## RAAB7 Cloud security

RAAB7 is hosted on a dedicated AWS Virtual Private Cloud. This provides a secure and isolated section of the AWS Cloud where we have complete control through advanced firewall role based security groups protected by multi-factor-authentication.

Security configuration is also validated against the Center for Internet Security AWS Foundations Benchmark, which ensures RAAB7 follows industry-accepted best practices to ensure high-level security configuration.

# Data protection compliance

RAAB7 is fully compliant with the EU and UK's General Data Protection Regulation (GDPR). The GDPR was created to regulate the use of personal data and its key principle is to protect individuals' data. The GDPR has set the tone for data protection internationally, creating a new global standard for regulations. Countries around the world are now adopting and aligning to the principles of the GDPR.

This means that the way RAAB7 survey data is managed, processed and safeguarded is in compliance with the guiding principles of data protection regulations across the globe. The RAAB7 Data Sharing Agreement (between the RAAB7 partner, Peek Vision and the London School of Hygiene & Tropical Medicine) provides RAAB7 partners with legal assurance that data will be processed in compliance with data protection regulations.

# ISO 27001 certification

Peek Vision, which developed and hosts the RAAB7 software, is an ISO 27001 certified organisation. ISO 27001 is an internationally recognised security management standard that specifies best practices and robust security controls. The certification requires the implementation of an Information Security Management System that ensures an effective and rigorous security programme which is reviewed and continuously improved over time.

Certifications are performed by an independent certified auditing body which provides assurance that Peek's security programme is in accordance with industry leading best practices.

# Security testing

RAAB7 software undergoes annual penetration security tests, conducted by a third party specialist security testing company. The purpose of these tests is to simulate cyber attack, detect any potential vulnerabilities, and verify that robust security mechanisms are in place to prevent unauthorised users from accessing data and infrastructure.

# RAAB7 security overview

## Servers

RAAB7 software is hosted on Amazon Elastic Compute Cloud (Amazon EC2) running AWS Linux 2. It provides a security-focused, stable, and high-performance execution environment to develop and run cloud applications. Security updates are tested and applied to all RAAB7 software environments as they become available.

## Device security

RAAB7 survey data is collected on Android mobile devices using the RAAB7 app. The app enforces security protection on the device that includes strong pin protection and Android full-disk encryption. This ensures all data collected remains secure in the event of the device being lost or stolen.

## Access controls

Each RAAB7 survey is individually isolated through logical separation (via access controls) ensuring strict data confidentiality. Access to your survey data is controlled via authorised user access controls protected via multi-factor authentication and enforced strong passwords. Every password is also checked to ensure it has not been compromised in a data breach.

## Encryption

Databases are held on AWS encrypted EBS volumes. This provides 256-bit Advanced Encryption Standard using a key managed under the Amazon Key Management Service. Further data backups on Amazon S3 are also encrypted. All RAAB7 data transferred between any device (smartphones, tablets, laptops via mobile app or browser) and servers are also encrypted.

## System monitoring & alerting

Server and database logs are continuously monitored in real time through Amazon Cloudwatch. Resource log configurations are automatically evaluated against approved and secure configurations. This enables automated alerting and simplifies compliance auditing, security analysis, change management, and operational troubleshooting.

## Threat detection

RAAB7 is protected with AWS GuardDuty. GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorised behaviour to protect access, workloads and data. The service utilises up-to-date threat intelligence feeds from AWS, CrowdStrike, and Proofpoint and continuously evolves through machine learning.

## Network security

Network access is strictly controlled via Amazon EC2 security groups, which provide a virtual firewall controlling all incoming and outgoing traffic. Security group configuration is protected with multi-factor authentication and enforced strong passwords.

## Disaster recovery

A detailed and annually tested disaster recovery plan is in place to ensure rapid and efficient recovery of servers and database volumes in the event of a major incident. During any potential recovery a standard set of procedures are followed to ensure the servers, applications and data are fully restored without error.

## Data storage & resilience

Data is stored in a MongoDB database. The database is replicated across two hosts in different AWS data centre locations, providing automated failover if one host becomes unavailable.

## Database backups

Automated database backups are taken four times a day via encrypted snapshots and stored through Amazon S3. Access to backups is strictly controlled, audited and monitored.

## Software testing practices

All new releases of RAAB7 software are subject to a formal release management process. This includes multiple levels of testing prior to implementation, including a separate and dedicated testing team. Testing is performed, reviewed and approved prior to changes being promoted to our live software environments.

**For more information please visit www.raab.world**

**Or contact enquiries@raab.world**

peek

INTERNATIONAL CENTRE FOR EYE HEALTH


v1.1 June 2022.