





Technical overview Coala Heart Monitor System

Introduction

The Coala Heart Monitor System enables automatic analyzes of ECG (Electrocardiogram) and PCG (Phonocardiogram). A user will measure their ECG and PCG using a Coala device that transmits data to an iPhone or Android app. The measurement data is processed and analyzed and then presented to the user in the Coala app. Measurements can also be monitored and analyzed by medical professionals through a web interface, the Coala Care Portal.

The Coala Heart Monitor System CE marked and approved by the FDA as a Class IIA and Class II medical device respectively. Coala Solutions is certified according to ISO 13485 and ISO 27001.

Infrastructure

The Coala Heart Monitor System is cloud-based and runs on a Microsoft Azure-based platform. The general infrastructure is shown in Figure 1.

Data is transferred from users app to Coala servers through a secure connection (HTTPS) and is validated by an API server before it is stored in a secure and encrypted database.

Coala utilizes an automatic tool for identification of deviations from normal sinus rhythms using Cardiolund ECG Parser, a CE-approved algorithm from Cardiolund, Sweden.

Data Storage

All data processed by Coala Solutions is stored on virtual servers managed by Microsoft Azure. Azure is ISO9001, ISO22301, ISO27001, ISO27017, ISO27018 and ISO27701 certified. Data from EU/European customers are physically stored in Microsoft Azure West Europe data centers
in Amsterdam (The Netherlands). The Coala Heart Monitor system is GDPR compliant. Data from US customers are physically stored in Microsoft Azure Central US data centres in Iowa (USA).

Technical security measures

Data transmission and storage is protected by several security measures, including but not limited to:

Authentication
- Salted and hashed passwords
- Strong password requirements
- Temporary session tokens for API access o The JWT Bearer Token implementation follows the RFC 7519 standard
- The integrity of the measurement data is validated with MD5 checksum
- Restricted access
- Two-Factor Authentication by SITHS, BankID and TOTP
- Audit log
- Access to Coala servers for SW and database maintenance and upgrades are restricted by IP addresses

Transportation
- Data transaction over HTTPS between user and server and between server and customer
- Secure Bluetooth
- SQL injection protection
- Regional server-side input validation
- Protections against cross site scripting and request forgery

Storage
- Firewall protected servers
- Data stored in encrypted databases, Microsoft Azure West Europe (EU customers) and Microsoft Azure Central US (US customers), with redundant back-up sites physically separated from production sites.
- Logging and monitoring of abnormal activity
- Backups via Geo-redundant storage (GRS)

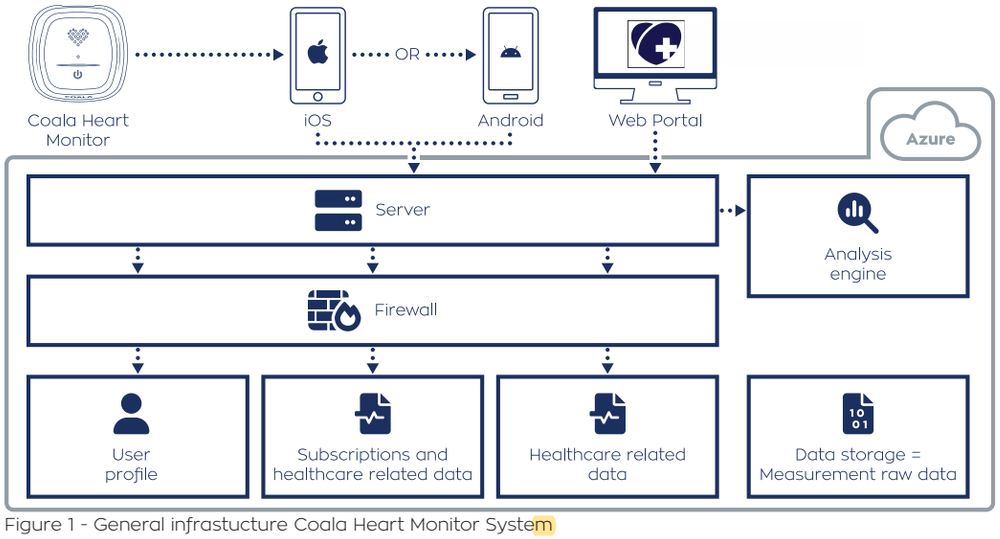


Figure 1 - General infrastucture Coala Heart Monitor System