CardioWatch 287-2 System Security Overview

Quality plan sign off	
Author: Ph. Fraboulet **Date**: 06-Feb-2023	**Reviewer**: P. Stas **Date**: 06-Feb-2023

Table of content

1 Introduction

The purpose of this document is to describe the Corsano CardioWatch 287-2 System (Corsano System) Platform Security. A secure and solid architecture has been crucial for the project. The Corsano System must guarantee performance and scalability, and provide Data Security and Privacy. Industry recognized best practices and Amazon Cloud Services (AWS) ensure that all necessary threats are considered.

The purpose the Corsano System is to provide a secure and reliable platform for vitals parameters continuous monitoring. The system is intended to gather, store, process and utilize data collected by the medical Corsano Bracelet and third-party medical devices.

The Corsano System includes a Cloud platform architecture and developed using Amazon Web Services (AWS) assets and functionalities. AWS supports security standards and compliance certifications necessary to implement secure and private medical cloud solutions (https://aws.amazon.com/compliance/).

The following topics are covered:

- System architecture
- Security and data privacy
- ISO compliance

2 System Architecture

The Corsano CardioWatch 287-2 System is comprised of:

- The Corsano CardioWatch 287-2B Bracelet (Abbreviated **Corsano Bracelet**)
- The Corsano App (Abbreviated **Corsano App**)
- The Corsano CardioWatch Cloud (Abbreviated **Corsano Cloud**)
- The Corsano CardioWatch Web Portal (Abbreviated **Corsano Web Portal**)
- Third-party external Medical Devices

The following schematic provides an overview of the Corsano CardioWatch 287-2 System:

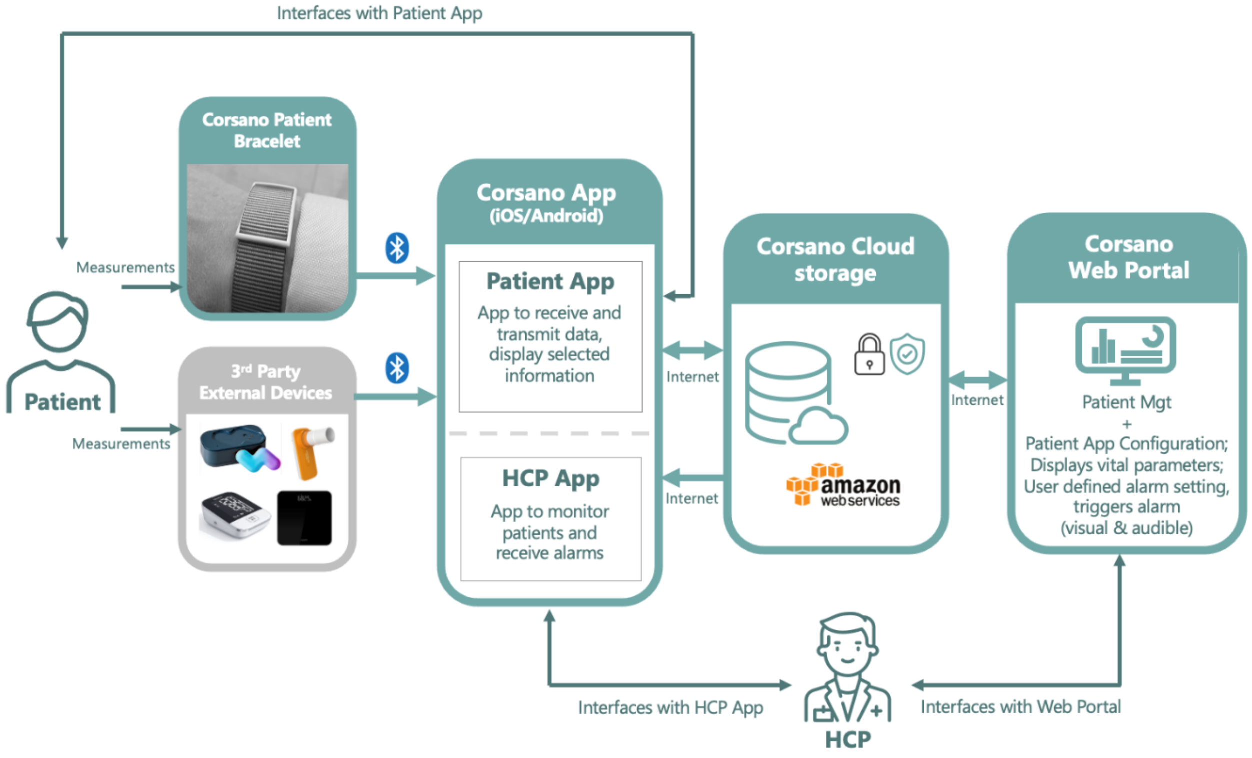
Interfaces with Patient App
Corsano Patient Bracelet
Measurements
Patient
3rd Party External Devices
Measurements
Corsano App (iOS/Android)
Patient App
App to receive and transmit data, display selected information
HCP App
App to monitor patients and receive alarms
Internet
Internet
Corsano Cloud storage
amazon web services
Internet
Corsano Web Portal
Patient Mgt
+
Patient App Configuration; Displays vital parameters; User defined alarm setting, triggers alarm (visual & audible)
Interfaces with HCP App
HCP
Interfaces with Web Portal

Figure 1 – Corsano CardioWatch 287-2 System overview

The Corsano Bracelet and third-party medical devices collect various vitals sign and physiological data such as Pulse Rate, SpO2, Respiration Rate, Temperature, Blood Pressure, Spirometry and Weight. The sensor data is first sent to the mobile phones and gateways via Bluetooth Low Energy (BLE) communication, and then delivered to the cloud through REST APIs over HTTPs.

Recorded data in the Corsano Bracelet is analyzed with algorithms to calculate the Vital Parameters that are reported by the system.

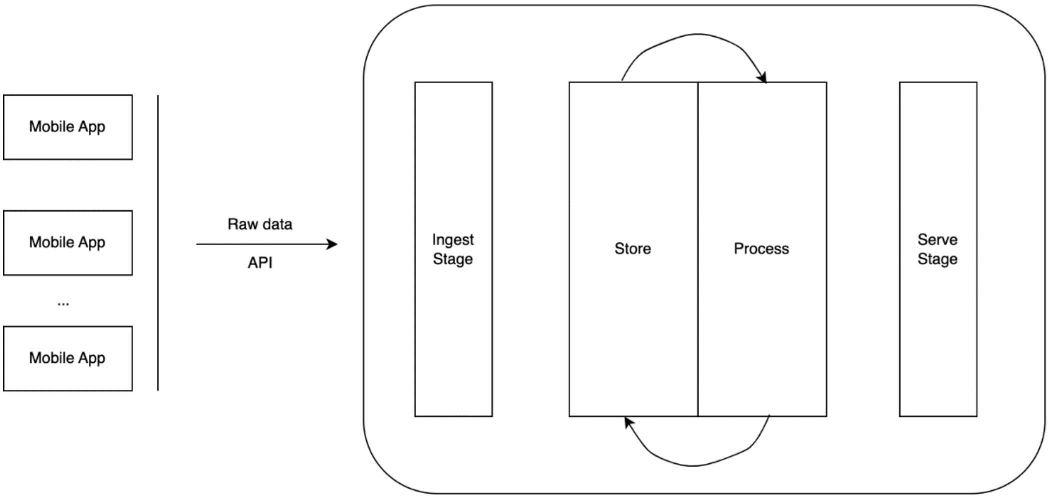

Figure 2 – Corsano Cloud Storage process

The Corsano Cloud is designed and deployed with AWS serverless architectures. Serverless architecture is an approach to software design that allows developers to build and run services without having to manage the underlying infrastructure. Cloud applications can be deployed and AWS services configured to manage the storage and scalability of the system.

Corsano uses serverless technologies provided by AWS and Atlas MongoDB such as EC2, S3, Elasticache, CloudWatch, IAM, KMS, etc.

- Data ingestion and storage: Atlas MongoDB, Corsano proprietary APIs.
- Data access: S3 archived files, Atlas MongoDB.

Daily backups of S3 instance and Atlas MongoDB databases are performed.

3 Security and Data Privacy

3.1 GDPR

The European Union’s General Data Protection Regulation (GDPR) requires companies to be accountable for how they use, manage and maintain the personal data of their customers and employees.

Corsano provides clients with enterprise-grade controls to manage, govern access and ensure security of personal data housed in the Corsano Health Cloud.

The company and the employees are fully aligned with the guiding principles of the GDPR regulation, bringing special care to Security and Privacy awareness, expertise of data processing legal basis, respect of the data subject’s rights, incident management procedures, accounting Data Processing Officers.

3.2 Security best practices

Security and Data Privacy is ensured at different level of the Corsano CardioWatch 287-2 System. AWS takes care of the physical, infrastructure and system level securities, by providing highly secured features and HIPAA compliant instances.

The Corsano System is also responsible for Security and Data Privacy. Role based data access with least privilege approach is managed with AWS Identity Access Management (IAM) and reduces the risks of intrusion. Corsano Cloud REST APIs are based on strong authentication technology and segregates Personal Information and Medical Information, to limit the risk of Data Privacy breach.

Data encryption is activated at all levels of communication, in transit and at rest. REST APIs use a high level of encryption (TLS1.2+). Data storage uses the industry standard AES-256 encryption.

The encryption keys are managed by AWS KMS, which is a fully centralized key management service that creates and manages cryptographic keys and control their use across a wide range of AWS services.

The data from sensor devices is sent to mobile devices via encrypted Secure BLE, using proprietary protocols, and then from mobile devices to cloud via SSL encrypted HTTP protocol. The data is stored locally in sensor devices, mobile, and cloud with various form of encryption following the policy of data encryption at rest. In the BLE transmission, the proprietary and private protocol adds an extra layer of encryption. Data packets are deciphered by the Corsano App to retrieve the vital parameters. In the HTTPs transmission, JSON is the used format to enable efficient operability.

3.3 Security of various layers

3.3.1 Corsano Bracelet

The Corsano Bracelet continuously measures Pulse Rate, SpO2, Respiration Rate and Skin Temperature. Data can only be accessed by BLE commands with Corsano private protocol. All BLE communications are encrypted with unique keys unique. Thus, data from Corsano Bracelet can only be retrieved by Corsano App.

3.3.2 Third-Party Devices

The External Devices can perform spot measurements of vital parameters and continuous measurement of axillary temperature. Compatible devices are FDA Cleared or FDA Listed and have a high level of security, ensured by secure Bluetooth Low Energy and private encrypted protocols.

3.3.3 Corsano App

Bluetooth data transmission is ensured by the application encrypted private protocol. The Bluetooth layer provides the Security Management (SM) Security, which can recognize BLE data encryption and decryption through key distribution. The underlying Bluetooth protocol uses AES 128-bit symmetric encryption algorithm. The 128-bit key length can provide sufficient security.

During Bluetooth pairing, key negotiation and key establishment are completed. In the first phase of pairing, pairs exchange pairing features. In the second stage, the key is generated. In the third phase, the Key is distributed. During the Key distribution, the Short Term Key (STK) or Long Term Key (LTK) generated in the second phase is used to encrypt links, preventing the Key from being directly intercepted.

After the pairing binding is completed, the paired dual-transmission communication links encrypt and decrypt packets according to the negotiated key. Even if the data packet is intercepted in the air, it is encrypted data.

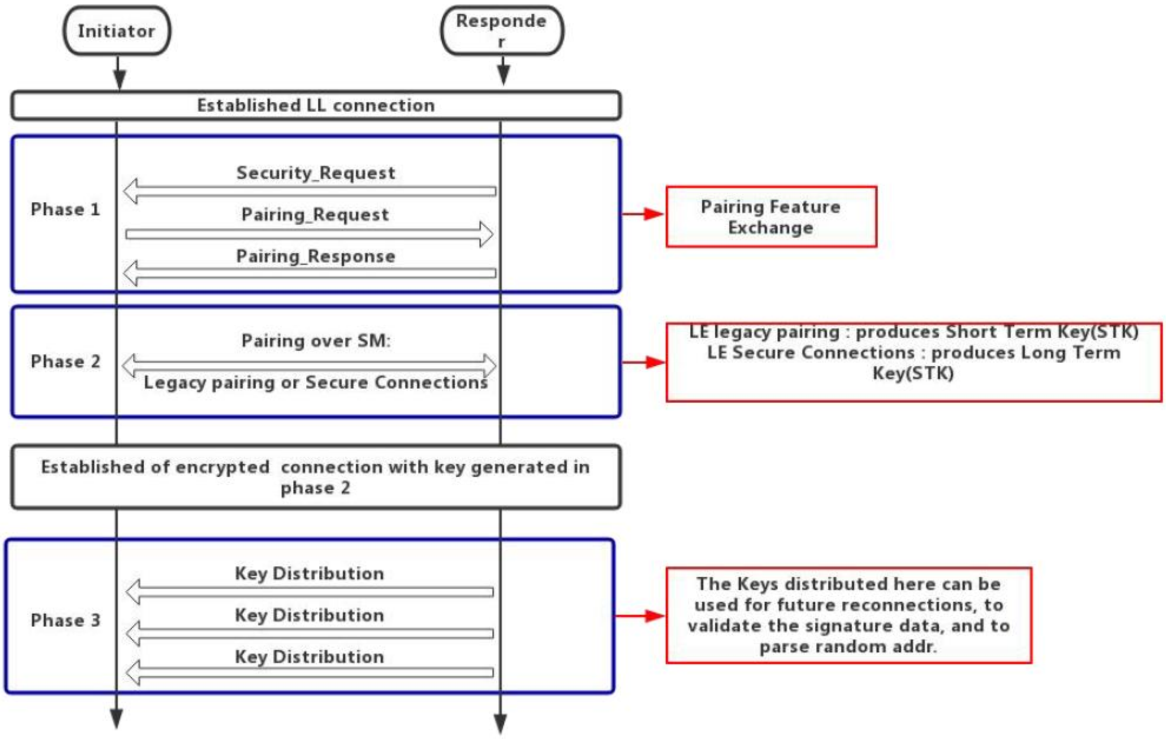
Initiator
Responde r
Established LL connection
Phase 1
Security_Request
Pairing_Request
Pairing_Response
Pairing Feature Exchange
Phase 2
Pairing over SM:
Legacy pairing or Secure Connections
LE legacy pairing : produces Short Term Key(STK)
LE Secure Connections : produces Long Term Key(STK)
Established of encrypted connection with key generated in phase 2
Phase 3
Key Distribution
Key Distribution
Key Distribution
The Keys distributed here can be used for future reconnections, to validate the signature data, and to parse random addr.

Figure 3 – Key exchange in Secure BLE protocol

When SDK sends data to cloud, it uses REST APIs with JSON data format. Data is sent via SSL protected HTTPS protocol.

3.3.4 Cloud (AWS)

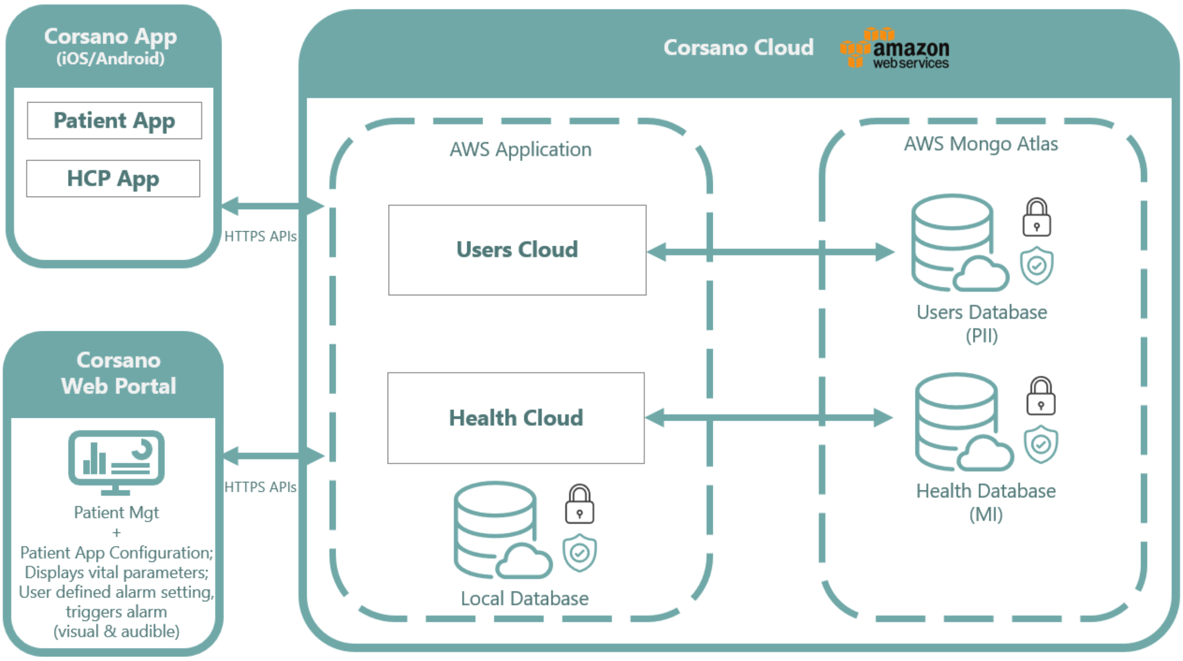

Figure 4 – Corsano Cloud overview

In the cloud, AWS Virtual Private Cloud (VPC), private subnet, security group and IAM are used to ensure network and system level security of the Corsano System. Data is stored encrypted in the private subnet that is only accessible through preconfigured channels and designated entry points.

For external access, bastion servers, firewalls and multifactor authentication ensure the security of communications.

Corsano Cloud APIs use authentication with JSON Web Tokens. Personal information. And Medical information are accessed through different APIs using Unique User ID (UUID).

3.4 Data privacy

Personal information and Medical information are segregated and stored in different storage entities. Medical information is pseudonymized and accessed with UUID.

Security and privacy policies, employee data security and privacy awareness, limited permissions, combined with data encryption under well controlled encryption keys, further enforce the protection of the data in the Corsano Cloud.

3.4 Compliance

Corsano conforms to:

- HIPAA & GDPR
- FDA 21 CFR part 11
- QMS with ISO 13485 certification
- ISMS with ISO 27001 certification

Corsano certified ISO 13485 Quality Management System (QMS) was upgraded to cover and comply with the ISO 27001 norm for Information Security Management System (ISMS). The ISMS Procedures and Policies are listed below:

Information Security Procedures

Document type	Document name	Version
Scope and policy of the ISMS	CORSANO Cybersecurity Policy v1.0 20210920	1.0
Roles, Responsibilities and Authorities	REC-153-1 ISMS Roles Responsibilities and Authorities	1.0
Risk Management Procedure	SOP-73-2 Risk Management Procedure	1.1
Procedure for the Control of Documented Information	SOP-42-1 Document and Record Control Procedure	1.2
Incident Management Process	SOP-63-3 Incident Management Process	1.0
Procedure for Internal Audits	SOP-82-2 Quality Auditing Procedure	1.2
Information Security Communication Plan	SOP-82-3 Reporting to Regulatory Authorities Procedure	1.1
Procedure for Management Review	SOP-56-1 Management Review Procedure	1.1
Procedure for CAPA	SOP-85-1 Corrective and Preventive Action Procedure	1.2
Information Security Objectives Plan	REC-162-1 Information Security Objectives Plan	1.0
Statement of Applicability (SoA)	REC-161-1 ISMS Statement of Applicability	1.0
Relevant Laws, Regulations and Contractual Requirements	SOP-72-3 Regulatory Compliance	1.1

Information Security Policies

Document type	Document name	Version
Access Control Policy	REC-151-1 ISMS Access Control	1.0
Asset Management Policy	REC-171-1 ISMS Asset Management Policy	1.0
Business Continuity and Disaster Recovery Plan	REC-181 ISMS Business Continuity and Disaster Recovery Plan	1.0
Cryptography Policy	REC-171-2 ISMS Cryptography Policy	1.0
Data Management Policy	REC-171-3 ISMS Data Management Policy	1.0
Human Resource Security Policy	REC-172-2 ISMS Human Resource Security Policy	1.0
Incident Response Plan	REC-174-1 ISMS Incident Response Plan	1.0
Information Security Roles and Responsibilities	REC-153-1 ISMS Roles Responsibilities and Authorities	1.0
Operations Security Policy	REC-181-1 ISMS Operations Security Policy	1.0

Physical Security Policy	REC-183-1 ISMS Physical Security Policy	1.0
Risk Management Policy	REC-182-1 ISMS Risk Management Policy	1.0
Secure Development Policy	REC-184-1 ISMS Secure Development Policy	1.0
Third-Party Management Policy	REC-184-2 ISMS Third-Party Management Policy	1.0

4 Test Plan

Corsano defined the strategy of testing for the security of the Corsano CardioWatch 287-2 System.

This test plan is part of the Cybersecurity strategy of Corsano and aims at testing:

- The Software developed and used by Corsano products
- The Corsano Products in their implementation, by evaluating the security of the accessible interfaces (Penetration tests)

Overview and Test Plan

Document type	Document name	Version
System Security Overview	REC-110-1 CardioWatch 287-2 System Security Overview 20230118	2023-01-18
Cybersecurity Test Plan	REC-110-2 CardioWatch 287-2 System Cybersecurity Test Plan 20230118	2023-01-18

Test reports

Document name		Date
Privacy and Security Audit Report	D-PRO-02-05 - Corsano Privacy and Security Audit Report 20230118	2023-01-18
Software Vulnerability Scanning	D-PRO-02-05 - Test Report - CardioWatch 287-2 System - Vulnerability Tests 20230116	2023-01-16
Penetration Tests	D-PRO-02-05 - Test Report - CardioWatch 287-2 System - Penetration Tests 20230120	2023-01-20
Secure Cloud Architecture Report	D-PRO-02-05 - Test Report - CardioWatch 287-2 System - Cloud Architecture 20230125	2023-01-25