codeBLUE iQ

Technical Manual

FORMAT HEALTH

Revised December 2, 2020

Notices

This document is provided for informational purposes only. It represents Format Health's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Format Health's products or services, each of which is provided "as is" without warranty of any kind, whether expressed or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from Format Health, its affiliates, suppliers or licensors. The responsibilities and liabilities of Format Health to its customers are controlled by Format Health agreements, and this document is not part of, nor does it modify, any agreement between Format Health and its customers.

CONFIDENTIALITY NOTICE

Table of Contents

1. Introduction 3

2. CodeBlue IQ User Guide & Best Practices 4
- Compatibility 4
- Configuring CodeBlue IQ 4
- CodeBlue IQ Software Updates 4

3. Data Collection, Patient Record & Discrete Data 4

4. Data Transmission, Storage, and Access 5
- Transmission of Data to CodeBlue IQ 5
- Transmission of the Patient Record to the EHR 5
- Storage and Deletion of Data 5
- Accessing Discrete Data 6

5. Technology Specifications & Policies 6
- CodeBlue IQ Technology Specifications 6
- Data Handling and Retention 7

6. Compliance & Security 7
- Cloud Hosting Provider 7
- Device Vulnerability Management 8
- Encryption and Security 8
- Data 8
- EHR Integration 8
- RevitalPro/CodeBlue IQ EHR Integration 9

7. Privacy Policy & Secondary Use of Data 10
- Format Health Privacy and Security Policy and Notice 10

1. Introduction

This document describes CodeBlue IQ: The RevitalPro companion web application for resuscitation documentation management and quality improvement analytics for in-hospital cardiac arrest events (also known as code blue events), developed by Format Health. Included in this paper are details pertaining to technical specifications of CodeBlue IQ, technology stack, electronic healthcare record (EHR) integration, HIPAA compliance, and CodeBlue IQ best practices. For information on how to use CodeBlue IQ, please refer to the CodeBlue IQ User Manual.

2. CodeBlue IQ User Guide & Best Practices

Compatibility

CodeBlue IQ web application runs on any modern web browser, though we recommend Chrome on a desktop computer as the preferred environment. We discourage the use of CodeBlue IQ on smaller screens, such as mobile devices or small tablet devices to ensure that the optimal size of icons appear, and text is sufficiently legible.

Configuring CodeBlue IQ

CodeBlue IQ can be configured to fit your organization's workflow needs. There are one-time configuration items at the time of CodeBlue IQ implementation, including electronic health record (EHR) integration and single sign-on (SSO) integration, that is completed by Format Health and your organization's IT team. In addition, there are simple organization settings, including organization name, user role assignment, and notification email sender address, that can be configured by a CodeBlue IQ Administrator.

For EHR and SSO integrations, the Format Health team works with your IT team to identify and roadmap what type of integration will work best for your organization. For details on these integrations, please refer to Section 5. Technology Specifications & Policies and 6. Compliance & Security.

Organization settings can be configured by the CodeBlue IQ Administrator from the Organization Setting menu in CodeBlue IQ. For notification emails, CodeBlue IQ uses SendGrid to deliver email reminders to the care team from the sender address entered in the Organization Setting menu. In order to avoid these emails from being filtered or flagged as spam emails, your IT team may need to set up sender authentication by adding DNS records to your hosting service.

CodeBlue IQ Software Updates

Continuous improvements will be made to the CodeBlue IQ software. When a new version of CodeBlue IQ is released, the update is automatically made available to you next time you log into CodeBlue IQ. For major version updates, you will be notified with a release note from Format Health.

3. Data Collection, Patient Record & Discrete Data

All data collected during the event is captured on the RevitalPro tablet device in three formats:

1. Discrete (structured) data
2. PDF Patient Record
3. PDF Quality Improvement Record

RevitalPro collects structured, discrete data during each code event. Throughout the code event, each confirmation of a documentation item stores the data locally on the device. If the device is connected to the internet, the data is also sent to CodeBlue IQ (the companion web application) and stored in a PostgreSQL database.

At the conclusion of the event, RevitalPro will also render two PDF records from the discrete data. The first is the Patient Record for immediate review, addendums, and signatures on the device. In addition to the Patient Record, RevitalPro will also render a Quality Improvement (QI) Record with information relevant for QI but not to be included in the Patient Record. Both of these records can be rendered from CodeBlue IQ once the record is submitted to CodeBlue IQ from the RevitalPro tablet device.

4. Data Transmission, Storage, and Access

Transmission of Data to CodeBlue IQ

As documentation items are entered into RevitalPro, discrete data are securely transmitted to CodeBlue IQ database via REST API if the device is connected to the internet. If the device is not connected to the internet during documentation, RevitalPro will automatically attempt to transmit the data once internet connection is established.

Transmission of the Patient Record to the EHR

At the conclusion of the event and completion of all required steps, the Patient Record created on RevitalPro is transferred to the EHR system into the patient's medical record where it is accessible via the EHR as either a PDF document or discrete data, depending on the EHR integration. If there is missing information preventing the transfer of the record to the EHR, the user can login into CodeBlue IQ web application and complete the remaining steps, such as entering the patient's medical record number (MRN), then submitting the Patient Record to the EHR.

Storage and Deletion of Data

All data from each event are locally stored on the device until the event record and data are successfully submitted to CodeBlue IQ web application and database. Once they have been submitted, the data remains on the device for an additional 48 hours as a failsafe measure. After 48 hours, the event data is permanently deleted from the device as a security measure.

On CodeBlue IQ database, the data is stored in a PostgreSQL database hosted on a secure, HIPAA-compliant hosting platform. Data is encrypted at rest using AES encryption with 256-keys. The data on CodeBlue IQ is stored indefinitely until termination of service. Please refer to your Agreement for details on termination and storage.

Accessing Discrete Data

All data and records from RevitalPro are available through CodeBlue IQ web application (so long as they have been properly uploaded from the individual device).

Authentication

RevitalPro and CodeBlue IQ system utilizes Auth0 authentication to protect information on the device, and to prevent unauthenticated pushes to the CodeBlue IQ database. We work with your IT team to integrate your organization's single sign-on process for a seamless authentication experience on RevitalPro and CodeBlue IQ.

Role-based Access

CodeBlue IQ uses role-based access control to streamline the workflow and limit security risk. These roles can be assigned by a CodeBlue IQ Administrator from the *Manage Users* page of CodeBlue IQ. In addition to manual role assignment, with SSO integration, we have the ability to map existing roles at your organization to CodeBlue IQ roles to automate the user role assignment process. As with SSO integration, we work with your IT team to map user roles.

5. Technology Specifications & Policies

CodeBlue IQ Technology Specifications

CodeBlue IQ Server	AWS + Healthcare Blocks
Application Framework	Ruby on Rails
Server OS	Ubuntu 16.04.6 LTS
Database	Postgres 9.5
Supported Authentication Protocols	OAuth 2.0 OpenID Connect SAML WS-Federation LDAP

Data Handling and Retention

ePHI data elements stored	Patient name Date of birth Medical record number Visit number Photographs
Length of time that records with ePHI will be retained on RevitalPro device	48 hours after transmission to the database
Length of time that records with ePHI will be retained on CodeBlue IQ database	Indefinitely, until termination of service per Agreement
Encryption mechanism for ePHI prior to transmission to server	TLS/SSL
Encryption mechanism for data at rest (server-side)	AES encryption with 256-bit keys
Database backups	Nightly snapshots of each disk volume. Monthly backups retained for 6 years by default.

6. Compliance & Security

Cloud Hosting Provider

Format Health hosts the RevitalPro backend, database, and CodeBlue IQ web application on Healthcare Blocks. Healthcare Blocks is a HIPAA-compliant application hosting platform, augmenting hardware and services provided by Amazon Web Services (AWS) to automate and enforce the requirements mandated under HIPAA. Please see your Agreement for more details.

Device Vulnerability Management

- Your computer's operating system and web browser should always be up to date with the latest version as these updates sometimes address vulnerabilities.
- If application-level vulnerability is found, the issue is fixed, tested, and an updated version of CodeBlue IQ is released as soon as possible.

Encryption and Security

- Hardened, secure Linux-based environment running on top of optimized Amazon Web Services hardware.
- Encrypted data volumes for storing database files and application logs using AES encryption with 256-bit keys.
- Restrictive access controls and persistent, extensible audit trail. Network access to virtual machines is inspected in real time and permanently logged. Intrusion attempts are automatically identified and blocked on a per IP address.
- Encryption of network traffic between nodes using strong TLS ciphers (insecure TLS ciphers are disabled).
- Redundant, 24/7 monitoring of uptime and resource availability.
- Intrusion detection system with automatic lockout of nefarious activity and frequent scans of filesystem for malware and rootkits.
- Automated database backups with rotation policies; disaster recovery process for production environments.

Data

- All data stored is safe and recoverable, protecting against accidental loss or mistakes.
- Disk volumes leverage a fault-tolerant, high-availability storage system.

- Nightly snapshots create a backup of each disk volume.
- For data integrity purposes, database backups are automatically enabled based on a consistent schedule, sensible rotation, and retention policy.
- Monthly backups are retained for 6 years by default.
- Database backups are encrypted and stored in a highly durable storage infrastructure (99.999999999% durability and 99.99% availability).

EHR Integration

Data from RevitalPro and CodeBlue IQ can be integrated into your EHR system. We utilize a HITRUST, SOC2-certified, and HIPAA-compliant integration platform to deliver seamless integration by establishing a secure VPN connection. This connection is continuously monitored to ensure exchanged data is always secure. We provide 3 different levels of integration depending on your integration needs and EHR capabilities:

RevitalPro/CodeBlue IQ EHR Integration	
Level 1	PDF document of the Patient Record attached to the patient's medical record.
Level 2	PDF document of the Patient Record, AND Discrete data from RevitalPro/CodeBlue IQ mapped to structured fields in the patient's medical record.
Level 3	PDF document of the Patient Record, AND Discrete data from RevitalPro/CodeBlue IQ mapped to structured fields in the patient's medical record, AND Integration with additional modules, such as medication administration record, laboratory orders, and billings.

Compatible EHR vendors include, but are not limited to:

- Allscripts
- Athena
- Cerner
- Commonwell
- Epic
- GE Healthcare
- Greenway
- McKesson
- Meditech
- Nextgen

- PulseCheck ED

Supported EHR messaging standards (TCP traffic encrypted via secure VPN connection) include, but are not limited to:

- HL7v2
- CDA
- FHIR
- Web API

7. Privacy Policy & Secondary Use of Data

Format Health's privacy policy covers the customer data and includes information about the customer business and employees.

Format Health does not utilize PHI from customers for any non-business purposes. Additionally, Format Health's privacy policy includes clauses addressing additional protections in different states.

Format Health Privacy and Security Policy and Notice

This privacy notice discloses the privacy and security practices of Format Health ("Company"). This notice applies solely to this company and its products, and pertains to Software-as-a-Service (SaaS) offerings to hospitals, universities, and other healthcare organizations ("Customers").

Privacy

This notice informs you of the following:

1. What personally identifiable information is collected from Customers through Company's software application, website, or other mechanism, how it is used and with whom it may be shared.
2. What choices are available to Customers regarding the use of Customer's data.
3. The security procedures in place to protect the misuse of Customer's information.
4. How the Customer can contact the company to correct any inaccuracies in the information.

Information Collection, Use, and Sharing

Company retains the right to utilize data gathered from Customers for its own purposes, so long as such use does not violate HIPAA, the Agreement with the Customer, or any other state or federal laws. No Protected Health Information ("PHI") shall be shared with third parties outside of the Company, except under a Business Associate Agreement ("BAA") as required in the ordinary course of business or as otherwise compelled by law. The Company adheres to privacy protections of each individual state where a Customer or Customer employee is located.

Unless you ask us not to, we may contact you via email in the future to tell you about updates, new products or services, or changes to this privacy policy.

Security

We take precautions to protect our products and Customers. Any sensitive information gathered via the Company's application or via other channels, is protected both online and offline. Only employees who need the information to perform a specific job are granted access to personally identifiable information or protected health information of the Customer or its patients. The computers/servers in which we store personally identifiable information are kept in a secure environment.

Our products are configured as HIPAA-compliant. We partner with industry leading third parties for cloud hosting services and compliance support, such as Healthcare Blocks. Some Customers may choose to institute on-premises hosting of the Server side of the application, in which case the references to cloud hosting and compliance are not applicable.

Data loss prevention (DLP) tools are implemented. On a quarterly basis, Format Health evaluates all third party libraries and software for security updates and patches, which are scheduled during regular maintenance windows. If a security event is identified and not corrected, our Customers will be notified.

Software as a Service (SaaS) Access

Format Health products are privately managed. In partnership with our third-party subcontractors, the Company controls the client application and application upgrades. The Customer (SaaS end user) has access to the core application from an iPad, and is able to access some features from the desktop, laptop, or mobile device.

For Customers utilizing Company's cloud hosting offering, data backups are stored offsite and are encrypted.

Contacting Us

If you feel that we are not abiding by this privacy policy, you should contact us immediately by using the information below:

www.formathealth.com
P.O. Box 1609
Vashon, Washington 98070

admin@formathealth.com
p: 406.242.4814
f: 206.203.0880