ReVital PRO

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

The contents of this document and any attachments and hyperlinks are intended solely for the addressee(s) and may contain confidential and/or privileged information and may be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.

Table of Contents

1. Introduction

This paper describes RevitalPro: The mobile solution for resuscitation guidance support and documentation for in-hospital cardiac arrest events (also known as code blue events), developed by Format Health. Included in this paper are details pertaining to setup and use of RevitalPro, required hardware, technology stack, electronic healthcare record (EHR) integration, HIPAA compliance, and RevitalPro best practices.

2. RevitalPro User Guide & Best Practices

Compatibility

RevitalPro software requires 9.0 or later. It is compatible with Apple iPad.

We recommend that the RevitalPro software be run on Apple iPad (9.7") device for optimized performance. These iPad devices allow ample screen space for effective and efficient use of the RevitalPro software. Due to the screen size and performance limitations, we strongly discourage the use of RevitalPro on iPad Minis and iPads manufactured before 2016.

Procurement of Devices

Please refer to the quote section of your agreement to determine whether hardware was included with the purchase of the RevitalPro license. If your organization is responsible for the purchase of the hardware and does not have a pre-existing Apple reseller account, Format Health recommends working with Zones to purchase hardware. Please email info@formathealth.com and we will gladly introduce you to a Zones Account Manager who is familiar with our recommended hardware solutions and can support the purchase, deployment, and maintenance of said devices, as well as the use of a Mobile Device Management (MDM) system (see below).

Mobile Device Management (MDM)

Mobile device management (MDM) is software that allows hospital IT administrators to control, secure and enforce policies on tablets, smartphones and other endpoints. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network. By enrolling RevitalPro devices into an MDM

system, selected users or administrators at the hospital are given the ability to remotely manage, track, and update the RevitalPro devices.

Please refer to the quote section of your agreement to determine whether or not MDM software was included with your license of RevitalPro. If MDM was not included and you need to purchase your own MDM, we recommend Cisco Meraki Systems Manager for its robust MDM capabilities, such as security policy enforcement, battery level tracking, and geolocation (organizations already utilizing MDM can, of course, choose to use their existing solution). If you are purchasing an MDM solution for the first time, you can manage the purchase and setup of the MDM through our Zones account manager (the same vendor who we recommend for the purchase of hardware). Please email info@formathealth.com for details and an introduction to the Zones account manager.

iOS Operating System Updates

Periodically, Apple releases updates to the iOS operating system for iPads. Updating iPads to a new release of iOS can take up to 2 hours and prevent the use of any apps installed on the device, including RevitalPro. Additionally, significant changes Apple makes to the iOS software can affect the performance of RevitalPro. If MDM was included with your license, we coordinate with your administrator and IT team to update the iPads to the latest iOS while minimizing downtime (e.g., staggering updates across devices). For customers using their own MDM and/or devices, updating the iPads to the latest iOS release is at the discretion of the user and/or hospital RevitalPro administrator.

Installation of the RevitalPro Software on Devices

Upon receiving the devices, they will be ready for installation of RevitalPro software via Apple Business Manager and Custom App distribution if not already installed. We will work with the on-site RevitalPro administrator to successfully install the software on the devices. Please refer to *Appendix - Purchasing Hardware and Installing RevitalPro Software* for details on hardware procurement and software installation.

RevitalPro Software Updates

Continuous improvements will be made to the RevitalPro software. When a new version of RevitalPro is released, the RevitalPro administrator will be notified along with details of the release and instructions on how to update RevitalPro on each iPad through their Apple Business Manager account.

Recommended Device Settings

If hardware was included in your RevitalPro purchase, the devices will already be configured to our recommended settings. If you are purchasing the hardware from Zones, or bringing your own devices, the below table describes our recommended settings for iPad devices:

ITEM	Setting Information
RevitalPro Standard Lock Screen	Standard locked screen guides user to press home button
RevitalPro Standard Home Screen	Standard home screen guides user to press RevitalPro icon
iCloud Account	Set to Institution's Apple Business Manager Account
Notifications	All OFF (Settings > Notifications)
Volume	MAX (Settings > Sounds)
Screen Time	OFF (Settings > Screen Time)
Multitasking Docking Stations	OFF (Settings > General > Multitasking & Dock > Lock Rotation)
Screen Orientation	Locked Horizontal with Home button on right (Quick Settings Lock Rotation BUTTON)
Date & Time	24-Hour Time; set automatically (Settings > General > Date & Time)
Display and Brightness	MAX (Settings > Display & Brightness)
Screen Auto-Lock	15 Mins (Settings > Display & Brightness)
Siri & Search	Remove all "asks" and "suggestions" in RevitalPro (Settings > Siri & Search)
Touch ID and Passcode	OFF, alternatively: a passcode set by institution (Settings > Touch ID and Passcode)
Camera used in RevitalPro App	Provide Permission by opening RevitalPro: take pic (1st time only)
Microphone used in App	Provide permission by opening RevitalPro: dictate (1st time only)
Remove unnecessary applications	Remove deletable iOS applications other than RevitalPro, Safari, Mail, and Settings.

Administrator Interface

The "RevitalPro Administrator Settings" allows users to access locally saved Patient Records. The administrator interface can be accessed by opening the RevitalPro app, and clicking the "Administrator Settings" button on the main page. The user will be prompted to enter their authentication credentials (*please see Section 4 - Accessing Discrete Data for details on authentication)*. Only users with the appropriate role and access level will be able to access the administrator settings. We work with your IT team to map RevitalPro/CodeBlue IQ roles with

existing roles at your organization. Furthermore, administrators can manually configure and manage roles and access via *Manage Users* tab in CodeBlue IQ.

Protective Cases

RevitalPro iPad protection can be achieved through the use of hard plastic, rubber combination cases. If the iPads you are using are on lease from Format Health, these cases will be included (if you are uncertain, please refer to the quote section of your agreement to determine whether or not the hardware was included with your license of RevitalPro.) If you are purchasing your own hardware, we recommend that you also purchase protective cases that feature a hand strap on the back of the case to increase comfort during the use of RevitalPro, such as BRAECN iPad Case with Hand Strap.This case can be purchased through our recommended Zones account manager at the same time as purchasing hardware and MDM solutions. Please email info@formathealth.com if assistance is required.

Tablet Battery Charging

Apple iPads are charged via the Lightning Port at the base of the iPad. Charging of the iPad can be achieved using Apple Lightning to USB cables and Apple 12W USB Power Adapter.

Apple Lightning to USB Charging Cable
Apple 12W USB Power Adapter

We recommend that iPads always maintain a 75% or greater charge in order to ensure they are ready for an emergency. Some MDM solutions enable the tracking of battery levels and we also suggest routine manual checks of the devices.

Tablet Cleaning and Sanitation

To ensure that RevitalPro iPads are sterile for use in the hospital, we recommend keeping the screen protector and case on then utilizing your existing methods and/or products for sterilizing other equipment to wipe down the iPad, case, and accessories. If you remove the iPad from the case for any reason, please ensure the sterilizing product is safe to use with the iPad prior to applying any products directly to the iPad.

If you do not have an existing sterilization process and product for other equipment, we recommend using either PDI Sani-Cloths with 2% CHG, or Clorox Disinfectant Wipes to sterilize the case, iPad, and accessories. Both products have been proven to be effective in disinfecting iPads from MRSA and VRE while also providing a residual antibacterial effect without damaging the iPad. [1]

For use in the OR, sterile, disposable cases designed specifically for tablets in the OR can be purchased. A link to guidelines for safe usage of electronic tablets in the OR can be found below. [2]

[1] "Disinfecting the iPad: evaluating effective methods."
[2] "Guidelines for Safe Use of Tablets in the OR."

3. Data Collection, Patient Record & Discrete Data

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

1. Discrete 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.

4. Data Transmission, Storage, and Access

Printing and Emailing the Patient Record

At the conclusion of the event, the PDF Patient Record rendered on the device can immediately be printed and/or emailed given wireless connectivity and an AirPrint-enabled printer. These features should only be used in line with hospital policy.

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 is 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 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.

5. Technology Specifications & Policies

Device & System Configuration

Device	Apple iPad
Application Framework	React Native
OS	iOS 9.0 or later
Supported Authentication Protocols	OAuth 2.0 OpenID Connect SAML WS-Federation LDAP
Database (server-side)	Postgres 9.5

Data Handling and Retention

ePHI data elements captured on the device	Patient name Date of birth Medical record number Visit number Photographs
Length of time that records with ePHI will be retained on the device	48 hours after transmission to the database
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

- We highly recommend enrolling devices in a mobile device management (MDM) platform to configure the devices to limit their use to RevitalPro, enable remote wipe, enforce passcodes, monitor location and battery level in order to minimize risk.
- Operating system (iOS) should always be up to date with the latest version as these updates sometimes address operating system vulnerabilities. Please refer to the *iOS Operating System Updates* section of this manual for details on updating the operating system.
- If application-level vulnerability is found, the issue is fixed, tested, and an updated version of RevitalPro is released as soon as possible. Please refer to the *RevitalPro Software Updates* section of this manual for details on updating the RevitalPro software.

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 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 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 mapped to structured fields in the patient's medical record.
Level 3	PDF document of the Patient Record, AND Discrete data from RevitalPro 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
admin@formathealth.com
p: 406.242.4814

Vashon, Washington 98070 f: 206.203.0880

8. Appendix - Purchasing Hardware and Installing Software

Purchasing Hardware

Hardware can be purchased through your company's pre-existing Apple reseller account. If your organization does not have a pre-existing Apple reseller account, Format Health recommends working with Zones to purchase hardware.
To set up a new Zones account, simply send an email to formathealth@zones.com that includes:

- the name of primary contact at your organization for the purchase,
- their email address, and
- their phone number

The Zones Customer Acquisition and Development Group (CAD) will contact the primary person and create a new account, and your Zones Account Manager will assist with the purchase of necessary devices (iPads, etc.) and accessories (Cases, etc.).

Once your hardware is received, your Zones Account Manager will provide instructions on how to set up an Apple Business Manager account for downloading the RevitalPro application. We also recommend RevitalPro devices be used with a mobile device management (MDM) system to optimize the functionality and security of mobile devices within the enterprise. If MDM was not included and you need to purchase your own MDM, we recommend Cisco Meraki Systems Manager for its robust MDM capabilities, such as security policy enforcement, battery level tracking, and geolocation.

Step 2 describes the Zones purchasing process in detail.

Installation of Software and Remote Management of Devices (MDM)

Upon receiving the devices, they will be ready to install the RevitalPro software via our mobile device management system, Cisco Meraki, or any other Mobile Device Management solution, which allows you to enroll and configure devices remotely.

RevitalPro downloads are provided to the organization through the Apple Business Manager. This will require a hospital device manager to create an account on Apple Business Manager.

Creating an account and registering the organization with Apple Business Manager is free of charge and your Zones Account Manager can help guide the organization if needed.

Apple Business Manager Setup

To set up an Apple Business Manager Account you must complete the enrollment process.

Follow these steps:

1. Go to Apple Business Manager
2. Click **Enroll Now**
3. Enter the following organization information:
    a. Data Universal Numbering System D-U-N-S Number
    Important: The D-U-N-S Number must match the legal organization name and address.
    b. Select your country or region
    c. Phone number (The phone number is pre-populated with information from the D-U-N-S Number. You can enter a new phone if necessary.)
    d. Website URL. **Important:** This domain is used to prepopulate Managed Apple IDs. However, if your organization website URL is different from your organization registered domain name, you can change it to your organization registered domain name before you create and assign Managed Apple IDs to other users of Apple Business Manager. *Note: You must use your organization's registered domain name in order for Managed Apple IDs to operate correctly.*
    e. Select your time zone and language
4. Enter and review your information:
    a. First and last name of the individual enrolling on behalf of the organization. *Note:* This must be a legal, human name. First and last names such as "IT Coordinator" or "iPad Deployment" will be rejected.
    b. A work email address that isn't associated with an iTunes or iCloud account, and that hasn't been used as an Apple ID for any other Apple service or website.
    c. Role/Job title
5. Enter and review the verification contact information. Apple will contact the verified contact to confirm your enrollment.
    a. Name
    b. Work email address
    c. Role/Job title
6. Click **Continue**, review the information carefully, then click **Submit**.
7. Check your email for a message from Apple Business Manager with the subject line "Your enrollment is in review."

During the review process, your verification contact will be contacted by phone and asked to confirm information about you and your organization before your enrollment is approved.

Make sure that any email filters allow mail from all apple.com domains, and return any missed phone calls quickly so the enrollment process can proceed smoothly.

Confirm Enrollment and Grant Administrator Access

After Apple confirms your information, that contact will receive an email message from Apple Business Manager with the subject line "Thank you for verifying your organization."

The contact will then complete the following tasks:

1. Open the mail message from Apple Business Manager with the subject line "Thank you for verifying your organization."
2. Review the message and do one of the following:
    a. Click the "Confirm [name of person]" button to let that person be an administrator of Apple Business Manager. This is the name of the person who initially enrolled in Apple Business Manager.
    b. If you don't want this person to be an administrator, click the "choose someone else" link, enter another person's information, then click Submit.
3. Your verified contact must also check the box indicating that you approve this person to accept responsibility for signing the Apple Business Manager terms and conditions on behalf of your organization.

After these tasks are complete, the person who was selected to be the administrator receives an email message from Apple Business Manager with the subject line "Enrollment Complete."

Create Managed Apple ID Account

Upon verification, you will receive an email message which will invite you to create your Managed Apple ID Account and to approve all the terms and conditions.

Follow these steps:

1. Open the mail message from Apple Business Manager with the subject line "Enrollment Complete."
2. Click the "Get Started" button.
3. Enter an email address for you to use as your Managed Apple ID. *Important:* This can be your work email address if you haven't used it as an Apple ID with an iTunes or iCloud account, or any other Apple services or websites. This email address becomes your Managed Apple ID.
4. Enter a secure password, then confirm it.
5. Confirm your name, then enter your date of birth.
6. Enter your SMS-enabled cell phone number, then select how you would like to obtain secondary verification.

7. Click **Submit**. Note: You'll be required to verify both your email address and your phone number.
8. Click the link in the mail message you received to verify your email address.
9. Enter the SMS verification code you received on your phone, then click **Verify**.
10. Accept the terms and conditions. *Note:* You must accept all terms in order to proceed.

Provide your Apple DEP ID to Zones and Format Health

Apple's Device Enrollment Program (DEP) is within Apple Business Manager listed as "Devices". The DEP ID is the Apple Business Manager account identifier that Zones will post device serial numbers which can be automatically enrolled under supervision with Cisco Meraki or any other Mobile Device Management solution.

Email your DEP ID to support@formathealth.com (and, if you have purchased through Zones, to formathealth@zones.com). This ID will be used by Format Health to "Whitelist" your organization to be able to download their App which is housed on the Custom App Store (Previously the B2B App Store).

Where To Find your DEP Customer ID

If you purchase devices from an Apple Authorized Reseller you also need to provide your DEP Customer ID to your reseller or carrier. Here's how to find it:

1. Log in to Apple Business Manager or Apple School Manager
2. Click Settings, then click Enrollment Information
3. Look for your DEP Customer ID in the Enrollment Information pane

Add Zones as a Device Supplier in Apple Business Manager

In Apple Business Manager:

1. Click **Settings** at the bottom of the sidebar
2. Click **Device Management Settings** below Organization Settings
3. Click **Edit** next to Customer Numbers
4. In the Reseller ID field, enter Zones' DEP Reseller ID: 10ABC70, then click **Done**. *Note:* If the Add button is missing or dimmed, this information may already be saved.

Enable Custom Apps to Install RevitalPro Software

1. Sign in to Apple Business Manager with an account that has privileges to manage system-wide settings.
2. In Content Manager click **Settings** at the bottom of the sidebar
3. Click **Enrollment Information** then **enable Custom Apps**.

You can now purchase any additional Custom apps from the Custom Apps section. Format Health's RevitalPro App is available in the Custom App Store to either be manually installed on each iPad by downloading redemption codes or installed via Cisco Meraki System Manager.

If you have any questions or need assistance, please contact support@formathealth.com.